

COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM (CAPPS II)

(108-55)

HEARING
BEFORE THE
SUBCOMMITTEE ON
AVIATION
OF THE
COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTH CONGRESS
SECOND SESSION

MARCH 17, 2004

Printed for the use of the
Committee on Transportation and Infrastructure



U.S. GOVERNMENT PRINTING OFFICE

95-120 PDF

WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

DON YOUNG, Alaska, *Chairman*

THOMAS E. PETRI, Wisconsin, <i>Vice-Chair</i>	JAMES L. OBERSTAR, Minnesota
SHERWOOD L. BOEHLERT, New York	NICK J. RAHALL, II, West Virginia
HOWARD COBLE, North Carolina	WILLIAM O. LIPINSKI, Illinois
JOHN J. DUNCAN, Jr., Tennessee	PETER A. DeFAZIO, Oregon
WAYNE T. GILCHREST, Maryland	JERRY F. COSTELLO, Illinois
JOHN L. MICA, Florida	ELEANOR HOLMES NORTON, District of Columbia
PETER HOEKSTRA, Michigan	JERROLD NADLER, New York
JACK QUINN, New York	ROBERT MENENDEZ, New Jersey
VERNON J. EHLERS, Michigan	CORRINE BROWN, Florida
SPENCER BACHUS, Alabama	BOB FILNER, California
STEVEN C. LATOURETTE, Ohio	EDDIE BERNICE JOHNSON, Texas
SUE W. KELLY, New York	GENE TAYLOR, Mississippi
RICHARD H. BAKER, Louisiana	JUANITA MILLENDER-McDONALD, California
ROBERT W. NEY, Ohio	ELIJAH E. CUMMINGS, Maryland
FRANK A. LoBIONDO, New Jersey	EARL BLUMENAUER, Oregon
JERRY MORAN, Kansas	ELLEN O. TAUSCHER, California
GARY G. MILLER, California	BILL PASCRELL, Jr., New Jersey
JIM DEMINT, South Carolina	LEONARD L. BOSWELL, Iowa
DOUG BEREUTER, Nebraska	TIM HOLDEN, Pennsylvania
JOHNNY ISAKSON, Georgia	NICK LAMPSON, Texas
ROBIN HAYES, North Carolina	BRIAN BAIRD, Washington
ROB SIMMONS, Connecticut	SHELLEY BERKLEY, Nevada
SHELLEY MOORE CAPITO, West Virginia	BRAD CARSON, Oklahoma
HENRY E. BROWN, Jr., South Carolina	JIM MATHESON, Utah
TIMOTHY V. JOHNSON, Illinois	MICHAEL M. HONDA, California
DENNIS R. REHBERG, Montana	RICK LARSEN, Washington
TODD RUSSELL PLATTS, Pennsylvania	MICHAEL E. CAPUANO, Massachusetts
SAM GRAVES, Missouri	ANTHONY D. WEINER, New York
MARK R. KENNEDY, Minnesota	JULIA CARSON, Indiana
BILL SHUSTER, Pennsylvania	JOSEPH M. HOEFFEL, Pennsylvania
JOHN BOOZMAN, Arkansas	MIKE THOMPSON, California
CHRIS CHOCOLA, Indiana	TIMOTHY H. BISHOP, New York
BOB BEAUPREZ, Colorado	MICHAEL H. MICHAUD, Maine
MICHAEL C. BURGESS, Texas	LINCOLN DAVIS, Tennessee
MAX BURNS, Georgia	
STEVAN PEARCE, New Mexico	
JIM GERLACH, Pennsylvania	
MARIO DIAZ-BALART, Florida	
JON C. PORTER, Nevada	
VACANCY	

SUBCOMMITTEE ON AVIATION

JOHN L. MICA, Florida, *Chairman*

THOMAS E. PETRI, Wisconsin	PETER A. DeFAZIO, Oregon
JOHN J. DUNCAN, JR., Tennessee	LEONARD L. BOSWELL, Iowa
JACK QUINN, New York	WILLIAM O. LIPINSKI, Illinois
VERNON J. EHLERS, Michigan	JERRY F. COSTELLO, Illinois
SPENCER BACHUS, Alabama	ELEANOR HOLMES NORTON, District of Columbia
SUE W. KELLY, New York	ROBERT MENENDEZ, New Jersey
RICHARD H. BAKER, Louisiana	CORRINE BROWN, Florida
FRANK A. LoBIONDO, New Jersey	EDDIE BERNICE JOHNSON, Texas
JERRY MORAN, Kansas	JUANITA MILLENDER-McDONALD, California
JOHNNY ISAKSON, Georgia	ELLEN O. TAUSCHER, California
ROBIN HAYES, North Carolina	BILL PASCRELL, JR., New Jersey
TIMOTHY V. JOHNSON, Illinois	TIM HOLDEN, Pennsylvania
DENNIS R. REHBERG, Montana	SHELLEY BERKLEY, Nevada
SAM GRAVES, Missouri	BRAD CARSON, Oklahoma
MARK R. KENNEDY, Minnesota	JIM MATHESON, Utah
BUD SHUSTER, Pennsylvania	MICHAEL M. HONDA, California
JOHN BOOZMAN, Arkansas	RICK LARSEN, Washington
CHRIS CHOCOLA, Indiana, <i>Vice Chairman</i>	MICHAEL E. CAPUANO, Massachusetts
BOB BEAUPREZ, Colorado	ANTHONY D. WEINER, New York
STEVAN PEARCE, New Mexico	NICK J. RAHALL II, West Virginia
JIM GERLACH, Pennsylvania	BOB FILNER, California
MARIO DIAZ-BALART, Florida	JAMES L. OBERSTAR, Minnesota
JON C. PORTER, Nevada	<i>(Ex Officio)</i>
VACANCY	
DON YOUNG, Alaska	
<i>(Ex Officio)</i>	

CONTENTS

TESTIMONY

	Page
May, James C., President and Chief Executive Officer of the Air Transport Association of America, Inc.	36
Mitchell, Kevin, Chairman, Business Travel Coalition	36
Ney, Hon. Robert W., a Representative in Congress from Ohio	9
Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, U.S. General Accounting Office, accompanied by David Powner, Director, Information Technology Issues, U.S. GAO	10
Rosenzweig, Paul, the Heritage Foundation, Senior Legal Research Fellow	36
Sobel, David, General Counsel, Electronic Privacy Information Center	36
Stone, Hon. David M., Acting Administrator, Transportation Security Administration, Department of Homeland Security	10

PREPARED STATEMENTS SUBMITTED BY MEMBERS OF CONGRESS

Berkley, Hon. Shelley, of Nevada	49
Costello, Hon. Jerry F., of Illinois	50
Johnson, Hon. Eddie Bernice, of Texas	52
Oberstar, Hon. James L., of Minnesota	72
Pearce, Hon. Stevan, of New Mexico	76

PREPARED STATEMENTS SUBMITTED BY WITNESSES

May, James C	55
Mitchell, Kevin	68
Rabkin, Norman J	78
Rosenzweig, Paul	101
Sobel, David	120
Stone, Hon. David M	135

SUBMISSION FOR THE RECORD

May, James C., President and Chief Executive Officer of the Air Transport Association of America, Inc., responses to questions	65
Stone, Hon. David M., Acting Administrator, Transportation Security Administration, Department of Homeland Security:	
Responses to questions from Rep. Berkley	144
Responses to questions from Rep. Johnson of Texas	146

ADDITIONS TO THE RECORD

American Society of Travel Agents, Inc., Paul M. Ruden, Senior Vice President, Legal and Industry Affairs, statement	148
Association of Corporate Travel Executives, Nancy K. Holtzman, Executive Director, statement	151
Business Travel Association of Germany, statement	154
Institute of Travel Management, statement	155
Practical Nomad, Edward Hasbrouk, statement	156
PrivacyActivism, Deborah Pierce, Executive Director, and Linda Ackerman, Staff Counsel, statement	159

STATUS OF THE COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM (CAPPS II)

Wednesday, March 17, 2004

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON AVIATION, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE, WASHINGTON, D.C.

The subcommittee met, pursuant to call, at 10:10 a.m. in room 2167, Rayburn House Office Building, Honorable John L. Mica [chairman of the subcommittee] presiding.

Mr. MICA. Good morning. I would like to call this hearing of the House Aviation Subcommittee to order.

Welcome everyone this morning. The topic of discussion at this hearing is the status of Computer-Assisted Passenger Prescreening System, CAPPS II.

The order of business is going to be opening statements by members and then we have two panels of witnesses. We will hear from our witnesses when assembled.

So, with that, I have an opening statement and then I will yield to other members.

First of all this morning, let me say that I personally strongly favor developing a passenger profiling system. However, with one big caveat, of course, that that profiling system does not discriminate unfairly or invade or abuse privacy.

Unfortunately, however, millions of Americans who travel by air each year are currently subjected to a passenger profiling and screening system that just lacks common sense. There is something very seriously wrong when we have a passenger profiling system that confiscates wedding cake knives and takes sewing scissors away from little old ladies and harasses children and Medal of Honor veterans.

We currently have in place what I call a Las Vegas roulette passenger profiling and screening system whose chances of detecting a terrorist are less than finding, unfortunately, a needle in a haystack.

There is no question that this system that we have in place now clearly needs to be changed. It must be altered to be effective and it must be altered to also narrow the focus to identify people who pose an actual threat to aviation.

We urgently need a passenger profiling system that identifies terrorists or bad people and at the same time does not discriminate or violate personal privacy. I believe that can be done.

However, our efforts to get there have been lagging. For sometime now we have been promised the CAPPS II is on the way, that CAPPS II is on the way. Unfortunately, it is not here yet.

However, CAPPS II is an important step toward addressing the problems by focusing attention on passengers with the higher probability of risk. That is what we have got to do with this system is focus attention on passengers that do in fact pose a risk.

According to the Transportation Security Administration, under CAPPS II, if and when we get it fully developed and deployed, an estimated 1 to 3 percent of passengers will be selected for an additional checkpoint screening, compared to about 15 percent of the passengers selected under this current Russian Roulette, Las Vegas-style system.

People who actually pose a threat will be better identified. If we can better detect threats with CAPPS II, then it should be implemented in fact as soon as possible.

However, I am told that TSA is again behind schedule in developing CAPPS II for several reasons. First is due to a lack of passenger data that are needed for system testing. Unfortunately, I believe that is unacceptable.

I believe that TSA has sufficient authority under the authorizing law that we passed and this committee helped to develop to require airlines to provide data and that TSA should take action by rule or whatever authority that we invested in them to do so promptly. This issue must be resolved without further delay.

Several other issues must also be resolved before CAPPS II is actually used to screen passengers in a working system. Unquestionably, sufficient privacy protections must be in place. Data and records must also be secured, must be limited in nature and must not be retained any longer than necessary.

Next, and most importantly, the accuracy of databases used by CAPPS II must be verified. Many government databases contain incomplete and sometimes inaccurate information. A terrorist watch list may include a single last name common to many people, however with no other distinguishing information.

Additionally, I understand that immigration data which will also be used by CAPPS II is often inaccurate and sometimes difficult to correct. Database accuracy is a significant challenge to the successful implementation of a CAPPS II program.

Third, a real passenger advocate and appeal process must be established for passengers who are erroneously selected by the system. American citizens must be able to correct inaccurate information contained in the various commercial and government databases that will be used by CAPPS II.

Finally, the effectiveness of CAPPS II algorithms must be proven. If CAPPS II becomes the threshold that identifies the passengers on whom all additional screening attention is focused, then our entire screening system will only be as effective as CAPPS II is designed.

If a terrorist fools CAPPS II by identity theft or some other method, then he or she will not be subject to additional security scrutiny beyond the basic checkpoint screening. That is why better screening technology is still absolutely critical to improving aviation security.

I might inject here, too, Mr. LoBiondo invited me up to visit Atlantic City on the morning of Monday, the 29th. That morning I have set aside to be in Atlantic City and look at some of the prob-

lems we have had in developing screening technology and also certifying screening devices.

Any of the members are welcome to join me on that occasion. I think it is an important meeting.

While CAPPS II has the potential to be helpful as part of a layered system of security, it must not be a substitute for deploying more effective passenger and screening technology.

I also continue to be concerned about the lack of an integrated terrorist watch list. That critical watch list is long overdue. I think some of you may recall, we all agree, bipartisan, both sides of the aisle, when we developed the TSA legislation, that that was one of the first things that had to be done.

Unfortunately, I am reporting on today, St Patrick's Day, the 17th of March, 2004, we still do not have an integrated watch list. That critical watch list must be in place to make all this successful.

Integrating the various law enforcement and intelligence agencies watch lists is an important vital first step toward better coordination of all of our security efforts.

As recently as last month, the Department of Homeland Security staff could not give me a timeframe for when an integrated terrorist watch list would be available. That is a very sad statement.

I want to take this opportunity to emphasize again how important it is that this information be integrated and available now.

In summary, I think that CAPPS II has the potential to significantly improve aviation security. However, it faces several challenges and must be implemented with care. I believe that open discussions of these challenges today will not only lead to an improved CAPPS II system and passenger profiling system that we can use, but will also help the system gain public acceptance and also answer many of the questions and concerns that have been raised.

I think this is also appropriate in that GAO just several days ago released this report, Aviation Security Computer-Assisted Passenger Prescreening System Faces Implementation Challenges.

We rely on GAO to do some of this work in looking at how this project from a technical standpoint is progressing. We will have questions from that report that I think we will all want to hear answers about.

So, I look forward to the discussion today and to the testimony of our witnesses who I think represent a good range of positions and experience and knowledge on the issue.

Those are my opening comments. I am pleased now to yield to our ranking member, Mr. DeFazio.

Mr. DEFazio. Thank you, Mr. Chairman. You know, Mr. Chairman, the CAPPS II system had promised that it was going to provide us with extraordinary security at low cost and instead it has provided us with cost without security, with no discernible progress.

To me, it is kind of like what we are doing in deploying the Star Wars system, which does not work, to shoot down missiles that no one is ever going to shoot at us, while we are leaving our borders open, our ports open to someone smuggling in a nuclear device in a truck or a container.

The same thing here: We want to go with this fix that will be able to assess the threat magically of every passenger and then

just screen those few people, lowering the burden on the workers at the airport, the TSA people.

But I have doubts that it is ever going to overcome the obstacles before it, not only technological, since this administration has thus far failed to merge the existing 11 or so lists that are out there into a workable single list so we can at least look at something to identify who are threat persons that are known.

That has been a couple of years in the making. That has not happened. But now we are going to have this whole new construct that will take anybody from anywhere in the world that is getting on an airplane and somehow magically assess whether or not they are a potential threat and merit more screening.

It's better to improve the screening at the airport, which we are not making a lot of progress on. I was just reading about experimental portals that are going to be used for groundside personnel at JFK that have been used in prisons and it says in the story that they found more contraband in one weekend than they found in a year at that prison from people going in and out.

But we have heard, we can not use portals because they would expose people's bodies or an outline of their body and everybody would be embarrassed.

Well, you can use stick figures. You can give everybody Arnold Schwarzenegger's body, whatever you want to do. You could have a computer simulation, but it would just show where the threat items are.

We are not doing anything to detect bombs, plastic explosives at the check point or on people's bodies. Did anybody at TSA ever hear about suicide belts? They are widely available and in use. Without embedded metal items to cause wounding when you only intend to kill or take down a plane, they would be totally undetectable with the current system. It is only a matter of time.

So, we play around, wasting money on this. I understand Lockheed is a defense contractor and this is the way they usually work, you know, 10 or 20 times over budget, five years behind schedule and no discernable product. But then sometimes it ends up like the Comanche helicopter where after wasting billions of dollars we cancel the darn thing and we are no further along.

I think that's where CAPPS II is headed. I have asked any number of times, any number of people in Admiral Stone's and his predecessor's place, what about a system that we could have implemented two years ago, last year, last month, today, Trusted Traveler?

There would be no cost to the government. People would pay for their own background checks. They would get an ID card that would allow them to use an express line. They would still go through the same minimal amount of screening we provide now, but they wouldn't be pulled out for random checks.

That happens to take a very small number of people who constitute a very large percentage of the daily passenger traffic because business travelers are small in numbers, but occupy, on a weekly basis, a lot of the seats.

Then that would allow the TSA screeners to focus on the remaining unknown people and the unknown threats they represent. It would also help the airlines a lot because the airlines are losing all

their high-end customers because they do not want to put up with the uncertainty, the hassles like when I was an hour and ten minutes early at National a couple of weeks ago and found that the line was more than an hour and ten minutes long to get through security.

Most business people aren't going to put up with that when they have the alternative of an executive jet and that's where they are going. So, this would help the industry. It would help TSA. It would help security and it would allow us to focus on those unknown people while Lockheed continues to spend money endlessly for no product until we finally cancel the CAPPS II program or it falls from its own weight.

Thank you, Mr. Chairman.

Mr. MICA. I thank the gentlemen. We have been joined also by Mr. Ney, who is not a member of this committee. It is the custom of the committee to grant, by unanimous consent, participation and sit-in rights to Mr. Ney.

Mr. Ney, what we will do is, we go through the members and then you will have your shot. But, without objection, Mr. Ney is permitted to participate in this hearing.

Let's see, Mr. Shuster? Mr. Pearce? Let me get the members on this side then. OK, we have Ms. Norton. You are recognized.

Ms. NORTON. Thank you, Mr. Chairman. Mr. Chairman, may I say that I agree with you? We certainly need a system. I mean we were seeing in this country where there were 19 folks who just walked right on in and left the other standing in their wake.

But, as you indicate, we need a system that is compatible, minimally, with the American values. That does not appear to be this system. We need a system that makes it difficult for them, but not for us. I am not sure how difficult this would be for them because the system does not look like it would be very effective. But it's surely difficult for us and we look at the problems that still are outstanding.

The CAPPS II system seems to be collapsing before it's even tested. We have a real problem when the public votes no before you even have a program because the airlines have refused to cooperate because of the concern of the marketplace, their own public.

On the other hand, I cannot imagine what it's going to take to get the public to accept the screening that CAPPS II at least is offering.

If you look at the GAO report, you look at the problems that have been raised, the problems that were raised before, the problems that continue to be raised, you know, the assumption was that perhaps as many as a third of the public would need to be prescreened. Then it was down to 15 percent. Now it may be even smaller.

I recognize that no matter how small it is, we need to keep people from getting to this country who come to wreak havoc.

People are already being delayed in travel here and they are being very patient with it. I think this committee has done a very good job in, in fact, working with the TSA in the design of a system that essentially has Americans saying, you know, search me, do whatever you want to so that I can get through here. I understand why you are doing it.

We already have indications that they will never understand CAPPS II as it now exists. I mean the problems go from the most basic problem any American will have which is what are you going to do with my data? What are you going to do with my business? What are you going to do with my information?

You have to begin with privacy issues that remain unaddressed. Then, assuming you can even get through that, particularly, given the initial response from the public, there is the question of accuracy of information. It is very, very difficult.

You know, we think that the names of Arabs are all the same. I am here to tell you that the names of Americans are all the same. You are all named John Jones or Mary Smith.

Finding a system that is able to differentiate all of us is a heck of a challenge and one that CAPPS II has not begun to meet. Then, of course, if you have a perfect system, we are imperfect beings, so there will be mistakes.

Finding a fast way to correct inevitable mistakes is the sine qua non of having such a system at all. This raises all kinds of due process issues. Here we are trying to people simply through the line and we talk about due process issues.

We have got to find another simpler way to do this. I won't even get to timeliness. We are already saying to people who have exercised enormous patience; it's going to take you longer to get through. You used to be there an hour ahead. You have to be there two hours ahead. I cannot imagine the waste in productivity. But it has to happen because we have to protect ourselves and our country.

Now, add another issue, another layer and you got problems unless it goes very smoothly. I just think we thought about this problem long before in our heads, way before the technology to make it happen was available and way before we had the expertise to do it.

Meanwhile, we've got to figure out what to do. I think that our most profound problem now, if we correct all these problems, which seems not to even be close to happening, is will the public ever accept how the CAPPS II that has already introduced itself, what a terrible introduction.

Having been introduced that way, how do we backtrack and say, no, no, that is not us. CAPPS II is really something else. I remain a profound skeptic.

I thank you, Mr. Chairman.

Mr. MICA. I thank the gentlelady. Are there further opening statements? Mr. Pascrell?

Mr. PASCRELL. Thank you, Mr. Chairman. I associate my comments with yourself and the ranking member as well. I think it is important that we continue to hold open and public hearings on the issue of aviation security.

We started this right after September 11, 2001. The nature of these hearings has been very revealing. We have come to some results. You understand our impatience and the impatience of the public.

He have heard from a lot of critics on the CAPPS II program. The latest GAO report confirms some of those fears. That report is really an eye-opener to all of us.

Admiral Stone, the bottom line is that the TSA is going to have to do a much better job of assuring the public that CAPPs II does not begin to look like big brother.

We want security. We want to know if the passenger is going to commit an act of terror, obviously. We are trying to prevent those things, as we work with other nations in terms of our ports, even. We cannot do this alone. We cannot check everything that comes into the country. So, we are trying to get other nations to verify and certify what goes into these things before they come, go on ship and come over here.

So, cooperation is very critical to what all of us are doing. Cooperation may be harder to come by in the future.

You are two years old, and I believe you have done some very good things. But there are too many delays and problems still outstanding that make me question my confidence in your ability to implement the system in the near future.

After all, when the system is completed, it has to be implemented or it is just on paper. It is frustrating that CAPPs II would not be deployed overseas.

Secretary Ridge recommended that we cancel certain flights in Britain and France. We know that there is a threat posed by some foreign nationals traveling from European nations. I know you will have access to passenger data from European countries for testing. But I cannot see the effectiveness of a system unless the Europeans make it seamless with their data.

Here at home people will want to know what sources TSA is tapping and why they cannot see any information the government has on them. I think that is a very pertinent question in a democracy.

In terms of the data actually collected, CAPPs II will replace TSA in what I think is a Catch-22 situation. CAPPs II should not store information for too long or it would be creating the big brother scenario the public fears.

The need for data correction for passengers that trigger a false negative will require that some passenger information is stored so that it may be corrected. For how long?

I can only fear the outrage from those who register false, unacceptable risks and miss weddings and graduations, et cetera, sorting out what happened. These are but some of the many inconsistencies and inherent problems which must be remedied before I believe the Congress will let this program be deployed.

Frankly, I believe that we must choose our priorities wisely. Physically securing the airplane by checking every passenger, every piece of baggage and cargo for explosives and every employee with air side access seems to be, to me, to be a better use of resources at this time.

It is phenomenal that, Admiral, you have to go through a screening process to get on an airplane and I have to go like every other member of the public, which is rightful.

But employees at the airports do not go through any screening. Hundreds of thousands of employees walk in and out, off the tarp, off the runways every day with simply a chain around their neck. This is preposterous. It is unacceptable. It needs to be changed immediately.

You know that that's how things are put on airplanes, drugs; need I tell you? And this is how things are stolen from airplanes. We go through this. We just had a case on Long Island, you know it.

Admiral Stone, you have a tough job. I wish you well. You are up for the job. Please call on us to be helpful. Please understand our frustrations. But we are not going to let our frustrations get in the way of moving forward; are we?

Thank you.

Mr. MICA. I thank the gentlemen.

Mr. Boswell?

Mr. BOSWELL. Thank you, Mr. Chairman. I, too, appreciate your having the hearing.

Mr. DeFazio, I associate myself with what you said. I just met Admiral Stone yesterday. I am almost starting to feel sorry for him. But he looks like he is a warrior, so I think he will be OK.

We are asking a lot. You know, I guess I have to tell you, Admiral Stone, of the years I spent in the production of agriculture. So, I suppose that I would say this: I continue to be an eternal optimist. But I want us to move forward.

We talked about that on another subject yesterday about national and the same thing applies. So, I am very pleased. This is a hearing going on. I want to hear from you, so I will be short.

But again, it has been 30 months. We have done a lot of things. I appreciate that. The traveling public, most of them, appreciate it. I tell a little story. I was in Des Moines getting ticketed and so on. It was one of those days. Someone I had never met before came up with her husband and I could tell by the look on her face that I was going to get it. I got it.

She lit into me about missing her flight. I had the audacity, I said, well, what time did you get to the airport? Well, she got there 30 minutes early. I said, well, you know, we all know we have to get here a little earlier under these conditions. She turned to her husband and said, I told you he wouldn't do anything. He does not care. And away they went, you know? So, anyway, you probably get a lot of that, too.

You know, this CAPPS II has been under review and there are problems with privacy, due process, accuracy, overall effectiveness and so on. We have heard these concerns. I share many of them, but while it is being delayed, one of the key participants in getting the system up, I guess, is the air carriers. Apparently, they have had some objections providing data due to privacy concerns.

So, get your arms around it. Let's get something happening. I think we can do better. We have a lot of people being checked that have been already background checked and so on and so on.

You are one of them and many others that serve in the Congress as well as people across the country. You know, they have had clearances, top secret clearance checks, secret clearances checks and so on.

I would hope we could get something going. Thank you, Mr. Chairman.

Mr. MICA. I thank the gentlemen. If no other members of the Transportation Subcommittee seek recognize, I am pleased to rec-

ognize my chairman on the House Administration Committee. He does a great job over there.

Congratulations on the new signage around here. It's great. I can even find my way around after 24 years.

Mr. NEY. I still cannot find my way around Rayburn, but we will work on it.

Mr. MICA. Well, that is a challenge. I figured if we leave bread crumbs or cheese—I am pleased to recognize Mr. Ney.

TESTIMONY OF HON. ROBERT W. NEY, A REPRESENTATIVE IN CONGRESS FROM OHIO

Mr. NEY. Thank you, Mr. Chairman. I give you credit. You are a person, both publicly and privately, that stays on beam in the building up and you have led the situation we have on the signs.

Thank you, also, Mr. Chairman and members of the committee for giving me the ability for sitting on the subcommittee today. I appreciate the important hearing that you have on CAPPS II.

I am not going to go into a long situation, but I have some concerns regarding the CAPPS II program. I think TSA has worked very diligently under a tough situation since 9/11.

I am a little bit troubled by the plan to implement it. I am just concerned as a lot of people are about the privacy, but also just the potential for errors and what happens if you get the one flag and you are banned from there and it was a mistake. I know nothing is perfect, but as this progresses, it has just got to be thought out to the very nth degree.

So, I, like others who have commented today, have some definite concerns on it or also the possibility of wrong information. I know in the computer age that can happen. So, I know you have a tough situation ahead.

I just think that thinking this thing all the way through is going to be important.

One other thing in conclusion, too, I fly like other members and we hear from people. But I have called TSA and I have got to tell you, I have had responses from your staff, Admiral. So, I give you a lot of credit for that.

I think consistency, you know, what you do in Kansas City, if you have to show the ID at the gate or if you have to show the ID in one place, you should have to do it the same across the country. That is what I hear from a lot of people. At one airport you check in and you go down and you have the ID. Sometimes they have asked at other airports for ID at the gates.

That's one thing I have called TSA on. I think consistency, exact consistency at all airports where possible will also alleviate some of the frustration of travelers.

Thank you. Thank you, Mr. Chairman.

Mr. MICA. Thank you. Are there any additional opening statements?

Ms. Millender-McDonald, you are recognized.

Ms. MILLENDER-MCDONALD. Thank you, Mr. Chairman. Thank you so much. It is good to see all of our guests here today. I am happy to be here to listen to the witnesses about the status of the computer-assisted passenger prescreening system.

I do represent Long Beach and kind of on the periphery Los Angeles Airport.

It is good to see you, Mr. Stone.

It is important to recognize the growth of the Long Beach Airport and the need for ensuring that we have not only the screeners, adequate screeners, but the prescreening system. And so today's hearing, I am sure, will illustrate the modern need for this and the importance of it.

So, Mr. Chairman and ranking member, I am just happy to be here, rushing in from another meeting. I will listen to the witnesses and take copious notes. Thank you.

Mr. MICA. Thank you. I did get a chance to look at that Long Beach screening process which they are doing intense and portable facilities for the passengers. I think when you get off a plane you are not allowed to stay in the terminal. There is not enough room.

Ms. MILLENDER-MCDONALD. It was good to see you there, Mr. Chairman.

Mr. MICA. Are there any other opening statements this morning? If there are no further opening statements, we will go now to our witnesses. I thank them for their patience.

Mr. Stone, you get to do a double header yesterday and today. Admiral David Stone is the Acting Administrator of the Transportation Security Administration.

We also have Mr. Norman Rabkin. He is managing director of Homeland Security and Justice Division of the General Accounting Office.

They are accompanied by David Powner, director of information technology Issues at GAO.

So, welcome. If you have lengthy statements or material you would like to have made part of this hearing record, please request so through the chair.

First, we will recognize Admiral Stone. You are welcome, sir. You are recognized.

TESTIMONY OF ADMIRAL DAVID M. STONE, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION; NORMAN J. RABKIN, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY DAVID POWNER, DIRECTOR, INFORMATION TECHNOLOGY ISSUES, U.S. GAO

Admiral STONE. Thank you, Mr. Chairman and distinguished members of the subcommittee. Mr. Chairman, Congressman DeFazio, Mr. Ney and distinguished members of the subcommittee, it is an honor be representing TSA as the acting administrator this morning and addressing the issues related to the second generation Computer-Assisted Passenger Prescreening system known as CAPPS II.

This system, once fielded, will be a significant enhancement to our overall aviation security posture. In addition to providing a quantum leap in our ability to verify identification, the system will offer rapid and efficient means of comparing these names against known terrorist lists.

Of note, the terrorist screening center remains on schedule to bring the first version of the consolidated terrorist screening data-

base on line by March 31, 2004 and achieve full operational capability by the end of the year.

The ability of CAPPS II to also conduct a risk assessment that is intelligence-based is envisioned to reduce our number of selectees, these are the travelers that are selected for secondary screening, at our nation's airports from 16 percent to approximately 4 percent.

By this I mean that we have approximately 1.8 million passengers a day going through our airports. We are looking at about 300,000 of them as secondary screening selectees and it is envisioned that CAPPS II will reduce that number from 300,000 to 75,000, a significant reduction in the hassle factor for our passengers.

This is an important benefit of smarter, intelligence-based selective screening. Not only will we see a dramatic reduction in the hassle factor experienced by passengers, but the increased throughput at our checkpoints and thus the overall customer service experience will be improved greatly.

Having served as the Federal security director at Los Angeles International Airport and seeing firsthand the impact of the current CAPPS II system on the traveling public, I am generally excited about the prospects of how we can both enhance security and customer service once CAPPS II comes on line.

Secretary Ridge has provided the Department of Homeland Security with a vision statement that I talk about daily in our morning operations and intelligence briefing. The statement reads: Preserving our freedoms, protecting America, we secure our homeland.

The fact that preserving our freedoms comes first in that statement reminds us that we must ensure that we never jeopardize those freedoms and liberties that we all love so dearly as we go about our business of protecting America.

The statement gets to the core of who we are and what we believe in and was in fact the focus of last week's nationwide TSA privacy education week. I mention this because as we go about the business of testing and implementing CAPPS II we know full well that the privacy, redress and oversight aspects are critical to our success.

In order to have the trust and confidence of the American people, we must ensure CAPPS II meets the highest standard in each of these areas. There is an inherent goodness to CAPPS II that I believe will shine through as we examine the program more closely.

TSA welcomes the scrutiny the program is under because we understand the importance of getting it right. The delays in testing have not caused us to waver in our commitment to this program.

We are keen to move down the road of CAPPS II, but not if it means shortcuts or taking the most expedient path. There is too much at stake to rush ahead without the proper privacy, redress and oversight procedures in place and we are working hard to refine these programs and our policies to support testing.

I am confident we will move CAPPS II forward in a thoughtful manner and provide the American people a program they will be proud of, one in which their freedoms are preserved and our country is better protected against terrorism.

In closing, I would like to thank you, Mr. Chairman, for your outstanding support and that of the subcommittee members. I look forward to answering your questions today.

Mr. MICA. Thank you. I would now like to recognize Norman Rabkin with GAO. GAO has completed the report which I referenced in my opening statement. Welcome, sir. You are recognized.

Mr. RABKIN. Thank you, Mr. Chairman and members of the subcommittee. I have a longer statement that I would like to provide for the record.

Mr. MICA. Without objection, the entire statement will be made a part of the record. Please proceed.

Mr. RABKIN. I am pleased to be here this morning to talk with you about our recent report on the CAPPS II program. With me is Dave Powner, one of the directors of GAO's information technology team. Along with Cathy Barrick of my team who was out on maternity leave, Dave led the GAO team that reviewed TSA's design of CAPPS II.

My testimony today highlights three areas from that report that we issued last month. First we address the status of TSA's development of CAPPS II. Our bottom line was that TSA has not yet completed important system planning activities.

TSA is currently behind schedule in testing and developing the initial increments of CAPPS II, due in large part to delays in obtaining needed passenger data from air carriers.

Furthermore, the target date for testing the system with data from one airline has been postponed and the new date has not yet been determined.

TSA also has not yet established a complete plan that identifies specific system functions that it will deliver, the schedule for delivery and the estimated cost of the system's development and implementation.

Secondly, TSA has not yet fully addressed seven of the eight issues identified by the Congress as key areas of interest. One issue has been addressed. DHS has established an internal oversight board to review the development of CAPPS II. DHS and TSA are taking steps to address the remaining seven issues.

However, they have not yet first determined and verified the accuracy of the commercial and government databases to be used by CAPPS II; second, stress tested CAPPS II nor demonstrated the accuracy and effectiveness of all the search tools to be used;

Third, develop sufficient operational safeguards to reduce the opportunities for abuse by authorized users;

Fourth, established substantial security measures to protect CAPPS II from unauthorized access by hackers and other intruders;

Fifth, Adopted policies and internal controls to establish effective oversight of the use and operation of the system;

Sixth, identified and addressed all privacy concerns; and

Seventh, developed and documented a process under which passengers can appeal decisions the system will make about their risk level and correct erroneous information in the databases used by CAPPS II.

We made seven specific recommendations to TSA. For example, we recommended that TSA identify specific milestones for when CAPPS II should achieve incremental functionality and at what cost, and we recommended that TSA develop policies and procedures outlining how CAPPS II will provide passengers with the ability to access and correct personal data.

DHS generally concurred with our findings and has agreed to address the recommendations.

Finally, CAPPS II also faces a number of additional challenges that may impede its success. For CAPPS II to operate effectively, it needs data on foreigners who plan to fly on domestic U.S. flights and flights to the United States that originate in other countries.

TSA needs to develop internal cooperation to obtain these data. The European Union in particular has objected to CAPPS II using its citizens' data, although the EU and DHS officials have reached an agreement to use data for testing purposes, the EU wants to see how Congress' concerns about protecting privacy will be resolved before committing further.

TSA also needs to decide how far beyond its original purpose CAPPS II should go. TSA is considering expanding what started as a system to try to prevent foreign terrorists from boarding U.S. aircraft to include suspected domestic terrorists, persons with outstanding Federal and state arrest warrants and persons with expired VISAs.

Finally, TSA need to ensure that CAPPS II will do all it can to ensure identity theft in which an individual poses as and uses information of another individual cannot be used to negate the system's security benefits.

Mr. Chairman, this completes my oral statement. Mr. Powner and I will be glad to answer your questions.

Mr. MICA. Thank you. We will go ahead and start some questions.

First of all, Admiral Stone, you just announced March 31, 2004, completion of—can you tell us exactly what that is? Is it the first three integrated watch lists? What will be available on March 31st?

Admiral STONE. Currently, the terrorist screening center, after it had stood up operations, it gave State and local law enforcement access to over 50,000 foreign terrorist watch list entries for the first time. So, currently, the cop on the beat can call in and do that check.

Mr. MICA. But will we have an integrated watch list on that date, also?

Admiral STONE. On March 31st, the first version of its consolidated terrorist screening database will be on line on that date and it will achieve full operational capability by the end of the year. So, this is the first version of your consolidated database being on line.

Mr. MICA. From all agencies?

Admiral STONE. For all agencies to be able to access that, yes, sir.

Mr. MICA. That is all agencies accessing. But how about the data on bad people, potential terrorists, that is going to be all in that one list on the 31st?

Admiral STONE. In the first version, the reason why they have caveated that is they are going to grow that through the year and improve on that by the end of the year.

Mr. MICA. The beginning list, it will still not be all information from all agencies on bad guys?

Admiral STONE. Right, yes, sir, that's correct.

Mr. MICA. When do you think that will be complete; the 31st of December?

Admiral STONE. Full operational capability by the end of this calendar year.

Mr. MICA. OK. Well, operational and integrating the list, I don't want to play semantics, but the watch list will be fully integrated and available within the system by the end of the year?

Admiral STONE. That would be the definition of full operational capability, yes, sir.

Mr. MICA. OK. There are seven issues that were raised. Congress has expressed concerns. I think only one or two of our concerns have been addressed.

Do you want to go through the seven real briefly?

Admiral STONE. I can touch on those, sir, yes. The privacy issue, we have been working very closely with Newokana Kelly at the department related to privacy. The first issue was to inculcate within the organization as a result of the Jet Blue incident as well as our core belief that we need to ensure every employee is educated on privacy.

Thus, the nationwide TSA privacy education week. That item was kicked off last week and we believe deeply in that. We continue to enhance that so that we do not see recurrences of asking for data that would be inappropriate.

Mr. MICA. Let me interrupt you before you go on because I want to elaborate a little bit more. One of the problems is that you have had hesitancy—I won't say lack of cooperation—on the part of the airlines to participate.

Is that primarily a liability concern? Then, if you do one or two airlines, does that sort of have them stand out?

The second part of my question, and I alluded to this in my opening statement, is I thought we gave you enough leeway in the TSA bill, creating the TSA bill, to pass rules to deal with situations like that, to pass a rule that mandated providing you with that information or requiring their assistance and cooperation on this.

Admiral STONE. Sure. I think the airlines are, appropriately so, are sensitive to ensure that they are respecting privacy rights, that the issue of liability is certainly on their scope as an item of concern when we talk. Mr. MICA. We know that now. Do you have the authority that you need to get them to cooperate and also at least allay some of their concerns or deal with the liability issue?

Admiral STONE. We do have that authority and believe that.

Mr. MICA. Then why haven't you used it?

Admiral STONE. It is our intent to be using the notice of proposed rule-making along with an SD to allow the airlines then to have the appropriate notification through the NPRM to education the public, their passengers on that and then to compel that data with an SD.

So, that parallel effort is in our tool box and it is our intent to work with the department on the timing of when those will be promulgated.

Mr. MICA. And when?

Admiral STONE. After we have had those discussions within the department, that we have reassured the department that we have met the privacy oversight redress requirement.

Mr. MICA. CAPPS II is not going to go forward until we get the airlines to cooperate, to get the system tested and then to get the system finalized and deployed. So, when is all this going to happen? Can you give us a timeframe?

Admiral STONE. I would anticipate here in the coming months, the next couple of months, that we will be able to have a decision related to the promulgation of the NPRM and the SD.

Mr. MICA. Well, that just means further delays. That is not exactly the way we envision this. I see heads sort of agreeing with me. We did not envision it to take—I mean we are already two and a half years out and we envisioned some of this.

Again, you are a new kid on the block. You are not a kid, but a very new player at this level. We have had your predecessor, Admiral Lloyd before us. We have had McGaw before us. We have had the Secretary of Transportation before that.

We just want to see if this is going to go forward that it gets implemented as soon as possible. Well, I want to give you time to respond to the rest of the concerns. Can you proceed?

Admiral STONE. Yes. It is our intent also to be hiring a privacy officer this month to report to the DHS, the department's privacy officer as another initiative to ensure that we have the coordination between what is taking place at our Office of National Risk Assessment, those actions that are falling under the purview of ANRA and that we think that that will also result in an improvement in terms of our privacy attention and being in compliance.

Additionally, with regard to external oversight and internal oversight, we have been working within the department and at TSA on an aviation security advisor committee.

We envision two working groups for that. One will be focused on privacy issues and we will deal with operational and technical issues related to ensuring programs such as Radiant Trust, which is the program that is used to monitor the system, the network for improper access or intrusion.

This operational and technical oversight working group is being set up as we speak, along with the privacy working group and reporting on in under the Federal Advisory Committee Act. So, this energy being put forward to get the proper oversight in place is right now an item of interest for us.

We have had additional groups come in and visit with us, the Markle Foundation, Zoe Baird visited with us last week to provide value added to that process. But the concept of ensuring that we have proper oversight, both internal and external, is currently a high-priority item for us.

This month, we anticipate being able to then present to the department where we are on the standup of those working groups and move forward then to reinstall confidence that we have a plan on that and it's a good one.

The redress system is based on having an ombudsman and a passenger advocated designated and a process in place so that when an individual finds that they are being repeatedly selected as a secondary screenee during their transit through the airport, that they will have an opportunity then to contact TSA, the ombudsman and the passenger advocate and then we will have the capability to have a decision made at the TSA level concerning going in on that individual and then adjusting the criteria for that individual after we verify their name, date of birth, address to go into that and make these decisions, we think, in a rapid matter so that it is not a bureaucratic system of waiting forever to get a response.

Our goal is to have a redress system that has flexibility in it and speed and scratches the itch for the traveling public regarding frustrations over being selected repeatedly.

I will note that when you have a program that is envisioned going from \$300,000 to \$75,000 selectees, we do not envision that the reaction will be from the traveling public that they are being selected for more opportunities.

We think that that will be an issue that the numbers of people that call about being sent for secondary screening will not be a significant number.

The issue will be if we get a number of people that are referred to law enforcement. We believe that CAPPS II, right now in our nation's airports when you are on a no-fly list or you are having to be run against a paper copy by the airline, there is great frustration about that.

CAPPS II's envisioned, because of the fact that we will have gone from about very low, single digit probability of who you are at the airport to something in the area of 99 percent verification of ID, that when we run and name against known terrorists lists, that this problem of having large numbers of people complaining about why are they on that list will be reduced, not increased.

So, this redress system, we believe, that we have in place with passenger advocates and a rapid ability then to input into the system if we find that there are problems that come up, we think we have a good game plan for that.

From a program management point of view, currently this year we have expended about \$14 million on CAPPS II. That is what we have expended.

As a result of the GAO and our own assessment, we have put a program management approach on this. We have enhanced the programmatic of it, watching the flow of people, money and program because we, too, are sensitive to make sure that this does not become a program that expands and is done in a thoughtless manner.

We want to have attention to detail and where that money is going. We have facilities now at Annapolis Junction, which is the back-up for Colorado Springs, which is the back-up for our primary site for the Office of National Risk Assessment which is located at Annapolis Junction.

That has been stood up out in Colorado Springs. In fact, I will highlight that the Office of National Risk Assessment, since December when we went to orange, has been able to do a program separate from CAPPS II, which is cockpit crew vetting so that

these international flights that are coming into the United States, that we were able to quickly run that through a terrorist database to get another risk mitigator on who are these people that are flying on international cargo flights into the United States and departing the United States.

Part of that budget of the Office of National Risk Assessment is also under close scrutiny on our part because that was able to take place on a merchant call.

All of those factors, program management, oversight, redress and privacy are at the top of our list to ensure that we are in compliance and are able to report back to the department that we are on track and ready to move forward on a testing initiative.

The testing piece of this, as was pointed out by GAO, many of the reasons that we were not able to verify the system and databases has been the issue of getting test data has been one that we have been very careful and thoughtful about because of our respect for the privacy issues related to acquiring that data.

We have worked very closely with the European Union on this. In their sensitivity about wanting to be partners with us, they have agreed to the providing of P&R data for testing purposes, but first needs to have it ratified by parliament.

We find that that timeline for that ratification fits in with our current schedule and we are confident that we will be able to work with the European Union for not only the testing data which we believe should be done with both European as well as U.S. domestic data.

That concept we believe, strongly sends a message that we are going to be partners on this testing and we are told that the European Union will be very keen to see the results of the testing and how our Congress reacts to that for the final implementation part of that.

But that wide array of issues, be it the testing of the system, privacy redress or oversight, we think we are progressing well on that.

Mr. MICA. Well, I appreciate your response. It did take some time and I hope the members understand that that question is in response to all the concerns that have been raised by Congress, that you should address today.

Just finally, one quick question for Mr. Rabkin and GAO. Now Congress asked you to look at this system that is being developed, CAPPS II, for passenger profiling. Tell us today, do you think they should continue developing and fielding this system and does it have potential for success or are we wasting time and money, again based on your observation, the report here and what you have heard from TSA?

Mr. RABKIN. Mr. Chairman, I think Admiral Stone is right that the Congress mandated that there be this kind of a system. The current system in place is not providing the level of efficiency or effectiveness that is acceptable. Something better is needed.

We are concerned, however, that the system that is being planned, while in theory seems that it would be effective, that the basic testing of it and whether it can work and whether the concerns of the Congress can be met are still major unanswered questions.

So, while we think that it is appropriate to have something better than what is in place now, whether CAPPS II itself is the answer, I think depends on how well the system is able to be designed and implemented. And that still remains to be seen.

Mr. MICA. Mr. DeFazio.

Mr. DEFAZIO. Thank you, Mr. Chairman. First, Admiral, I would start off, when TSA does something right I like to compliment them. The chairman and I both expressed concern about the new fining program that was announced.

I went and personally checked your website and it was very unclear. From reading the website I had extraordinary concerns about whether it was being applied uniformly or arbitrarily. The people I met with told me it was very different than the website page you were presenting to the public and my staff revisited the site yesterday and that saw since my meeting the page has been revised and it is much more useful information for passengers in terms of who might or might not be subject to fines.

I want to compliment the people I met with who did address my concern.

Just to follow on the Chairman's line of questioning, it is my understanding in the statute, which we authored, that we gave very specific authority to TSA to issue security directives with no notice of rulemaking, no public comment, et cetera.

You are familiar with that?

Admiral STONE. Yes, sir.

Mr. DEFAZIO. OK. Why wouldn't you just use that authority with the airlines and I would suggest you would use it with all the airlines, even though you may only want to use the data from one airline so that none of the airlines are singled out in this process as they have been thus far, although that was voluntary.

But when you go mandatory, if it became known that you were only mandatorily getting the records of one airline, there might be repercussions for that particular airline from passengers who have concern about how the data is going to be used.

But if you get it from all the airlines, even if you weren't going to use it and you did it through an emergency rulemaking, we wouldn't have any further delay in this area. Couldn't we just do that?

Admiral STONE. That would be an option, too, sir. Our recommendation to the department is in order to instill the trust and confidence and to provide notification to passengers that we will be taking data and testing it as part of CAPPS II.

It is our belief that the notice of proposed rulemaking, since that signal that we are respecting that right to privacy and people can make decisions about that, in fact I would like to add that our approach will be that we want to get that out and then allow the airlines time to tailor their IT systems to provide us the data which we believe will take a couple of months to do that.

But also it will allow us time to go by with that notice of proposed rulemaking out on the street, so the traveling public knows we are going to be doing that testing and it is our intent and we recommend that when we do the testing we look at historical data, that we then say that we are going to start at a—pick a particular month and then go back and look at that month and then filter out

those items that would be during the actual operational test phase so that we are not in the business then of impacting on the actual operations of the day until we see what the impact will be.

Mr. DEFAZIO. Right. That is why I understood that you were essentially going to do a computer simulation, which is why I was suggesting you might do it an alternative way. Well, anyway, good luck with that.

Admiral STONE. Thank you, sir.

Mr. DEFAZIO. ID theft, it seems to me the Achilles heel of this whole system is a sophisticated terrorist and they seem to be quite sophisticated and that assumes an identity and that identity has no detrimental characteristics attached to it and they assume it in such a way that it is not going to trigger alarms.

I do not understand how we are going to deal with that unless you are going to develop as one of the subsequent people will testify, if you are going to develop a whole bunch of new criteria that you are going to ask the airlines to ask height, weight, color of eyes, et cetera.

Of course, that would be, again, self-declared on the part of the person who could already have developed this identity with that height, weight, et cetera. But in any case, the data you are going to get is going to be name, address, phone number, et cetera.

Does someone live at that address? Have they lived there for a while? Do they have whatever? OK, great. But is it that person? We do not have the foggiest idea, and we won't have the foggiest idea.

So, it seems to me, this is just a tremendous potential problem, even after we go through all of this, even after you ever do resolve the privacy concerns and the concerns of Congress and the logistical problems.

It seems like again, kind of like Star Wars. We are going to wait there with an effective system for missiles that are not coming. Meanwhile, someone sneaks under it with nuclear weapons in a container.

This is the same thing. Someone is going to sneak through the system with a valid, you know, with an ID card with a history and a background and all that, but it just happens that they are not really that person.

Admiral STONE. Our view is that today when you look at where we are on ID verification at the airport, presenting the driver's license—

Mr. DEFAZIO. Where you present it to someone who does not even work for TSA, who is paid minimum wage.

Admiral STONE. Yes, sir. This is going to be a quantum leap going from that low percentage of verification of ID with great ambiguity to a 99 percent level, determination of ID and then—

Mr. DEFAZIO. Yeah, but have you heard of ID theft and manufacture? You can buy passports on the street in Europe. In the U.S. you can buy driver's licenses at any college.

What are we talking about here? We have a system of national drivers' licenses that are easily counterfeited, what is our confidence level that that person is who they say they are or they have not assumed an identity. I do not get where we are.

Admiral STONE. We believe then the pulsing of those commercial databases, if your VISA card has been taken, will result in CAPPS II detecting that anomaly because the card will have been reported as stolen and that you will then have that ambiguity reflected in your score and you will go to a secondary screening.

Mr. DEFAZIO. I don't know much about this stuff. I am on Homeland Security. I am on this committee. I struggle with it. I read novels. You know, you go and find someone who is dead. You assume their identity, their Social Security number. You develop an address, use your visa card for a year or two. These are patient people.

I still believe the only way to deal with this is to have a bullet-proof or bombproof screening system for all passengers, all employees and all people who have access to the air side of the airport and keep the threat items out.

If you get a threat individual but they have nothing to act with, well then the other passengers will take care of them or the air marshals. So, I just do not think we are headed down a path here that is going to work.

If I could, I don't have that much time, we will perhaps discuss the ID theft issue again later. I have asked now a number of people from TSA and it is a point that Mr. Pascrell brought up, which is that we have observed at certain airports all of the airport vendor employees are routinely allowed to bypass security entirely and file in and out while you have over here the pilots, the flight attendant and all the passengers who are having their moustaches scissors confiscated, I am a moustache guy, or their cuticle scissors or whatever else.

But over here we have these unknown people wearing bulky jackets, carrying things, just walking in and out of the airport. I have asked now for months, I was told, well, it's not really common, and some airports are doing it and some are not. We observed it at Detroit. I have been told that we are trying to find out what airports allow that.

It seems one simple e-mail from you to all the FSDs that says, at your airport who is allowed access to the terminal without going through screening? Is anybody and if so, whom? We could have the answer. But I have been trying to get that answer for a year now, having observed it a year ago in Detroit with the chairman.

I cannot get the answer, although, for instance, I was at Portland last Thursday, flew in and I noted a pilot who walked up to the people at the exit for security and he said, hi, hi, and he carried his bag and walked around and went in.

I am pretty confident of pilots, but I didn't even notice that they checked his ID to see. Of course, we do not have uniform IDs. But anyway, he just walked around security while the lines went down the terminal with all the other people.

Now is that routine at Portland? I don't know. Where are we allowing who to bypass security? I hear in Chicago that the flight attendants have to go through security and all the other workers do not who are coming in on certain buses.

I mean the system is so loophole ridden, I am not sure again. We are investing all this stuff in CAPPS II and we have all these other

people who are just like avoiding the system altogether who are potential threats.

So, I would really like that list and it has been promised any number of times, but of course, it has not yet been forthcoming.

I think the chairman would like it, too. I don't know, probably, just so we would know.

Then finally, just to GAO, if you would like to address the ID theft. Secondly, is CAPPS I better than nothing? We were talking about wanting to get away from these 300,000 people a day. Well, I figured out about the one-way tickets. The terrorists did, too. It was published on the front of the newspaper.

So, they are going to buy round trips. If they do not have a lot of money, they will book in advance. So, the point is this is a stupid system and every once in a while I have to buy a one-way ticket. Then I get the big black S and I have to go through security. Is it better than nothing?

Mr. RABKIN. In terms of identity theft, I think you are right. I think there are problems. It may be the one percent that Admiral Stone referred to. It may be more than that. In terms of CAPPS I, to the extent that it keeps people off planes that ought to be off planes, then it is better than nothing.

Mr. DEFAZIO. Why is it better than nothing?

Mr. RABKIN. Just because it subjects some subset of people to more intense screening.

Mr. DEFAZIO. The more intense screening is probably an efficiency issue. It just takes a little bit longer. Everybody goes through screening. Everybody on an airplane has gone through that. To the extent that the technology works, then prohibited items are kept off of the airplanes.

Mr. RABKIN. Unless an employee who works at McDonalds in the airport carried a gun around and gave it to someone on the other side of security.

Mr. DEFAZIO. That is correct. So, go ahead. I am sorry.

Mr. RABKIN. Are there some immeasurable benefits as a deterrent, if it makes people feel more secure, is it worth the cost is a different question that we are not prepared to answer at this point.

It is the same question that could be asked of CAPPS II, of whether the benefits are worth the costs.

Mr. DEFAZIO. OK. Thank you. Thank you, Mr. Chairman. My time has expired.

Mr. MICA. Thank you. Mr. Rehberg, I think you are next.

Mr. REHBERG. Thank you, Mr. Chairman.

Admiral, the one issue that I have not heard addressed is specifically about the partnership, obviously, that has to be created with the airline industry.

I have not heard any discussion about any kind of a cost-benefit analysis that is done to try and talk about the cost to the airline industry to try to get your computer system to match with their computer system. Can it in fact work?

Will you receive cooperation from the airline industry or from the ticketing agency or expedience on the others? Could you address the cost as you perceive it?

Admiral STONE. Yes. We have a very close partnership with Mr. Jim May, the head of the ATA, who I believe you will be hearing

from him later this morning. In fact we now have a group that meets.

An agreement has been reached which TSA, ACI, AAAE and ATA to use the Boeing model in which we will be able to look at our nation's airports for three things. The three major projects we are looking at, one is the issue that Mr. DeFazio mentioned on access at our nation's airports.

What would be the cost to invest in guns, gates and guards versus the enhanced background checks that TSA proposes? Additionally, they are going to look at the growth of our Nation's airports, the ACI and AAAE and the airlines are obviously very close to that and they are going to advise us on how that should affect the shaping of our screener workforce.

So, this partnership is alive and well. When I have talked to Jim May and others in the airline industry about the costing of this and the fact that the government will take the system over, in the near term obviously, the cost to the airlines of retooling their IT and their software to be compatible with CAPPS II is of some concern.

But the mid-to long-term benefits of that, they no longer as an industry have to fund the system which we have mentioned here is not as efficient and effective. It is not the system that many of us really want. I think that has caused them to be very supportive of CAPPS II and they have said that.

Basically, they would like to move forward as quickly as possible on it and just make sure that the privacy and oversight redress is in place so that in face when we direct them to provide that data, that they are being good public servants for their passengers.

Mr. REHBERG. Thank you. My second question has to do with Part 135, the Air Taxi and Commercial Charter. The question is: I heard Mr. Rabkin from GAO talk about the expansion being a problem. I don't know if it is necessarily an expansion, but have you put up any kind of barriers or suggestion that those passengers are going to be checked in the same way or it this included in CAPPS II in your envisioning more security?

Any terrorist can go and charter an airplane and jump on there and do the same problem that we are talking about, the 300,000 that are being checked in our commercial airports.

Admiral STONE. Yes. The charter program that we have in place, currently it is not envisioned to incorporate that into CAPPS II and our current program that we have in place for the 12(5) program and other measures that we take, that is our current plan for security for those type of aircraft.

Mr. REHBERG. Mr. Chairman, I won't ask any more questions so somebody else can ask them.

I want to thank you for staying on this issue. You know, I haven't been on the committee that long, just three years, but I do remember the debate after September 11th. A lot of fingers were pointed at the FAA for not having the screening, the testing, the penalties.

You in Congress said do it in 1994, do it in 1995. They never got around to it. I am hearing a lot of the same kind of bureaucratic mumbo-jumbo of not getting this thing done. So it is going to be incumbent upon you as chairman to stay on top of this.

I thank you for this hearing and for your continued interest.

Mr. MICA. Thank you. Ms. Norton.

Ms. NORTON. Thank you, Mr. Chairman. Admiral Stone, I would say I am glad to see you again. I am not so sure you are glad to see me or this entire committee again, two days in a row, but we certainly appreciate the way you responded yesterday.

For you and Mr. Rabkin, I do have a question about horror stories and liability because my own concern is that we may have failed to solve the problem at the testing gate.

Let me do that, you know, coming out of my own discipline as a law professor by giving you a hypothetical. You know, Eleanor H. Norton has an important business deal. So she goes to get on a plane and she is stopped. She is stopped because there is another Eleanor H. Norton, Washington, D.C.

Now, you have different addresses, presumably for these two Eleanor H. Norton. It says Eleanor H. Norton, let us say, Arab-American, Washington, D.C. You have perhaps different addresses. Is that going to be enough for Eleanor H. Norton to get on a plane so that she does not miss this million dollar deal or are you going to need to look beyond the addresses and if she does miss, who should pay?

I think that the reason that the airlines are fearful of doing anything, and as their lawyer I would have told them do not touch this. If you mandate this on them, I would say sue them to keep from having to comply.

So, how do you deal with Eleanor H. Norton, Arab-American. Here she is not on vacation. That will just make her real mad. But here you can give her real losses, one. How much does she have to go through so she can make that plane?

Do you really envision that she can make it with an identical name, and two, if she misses it, what should be the liability?

Admiral STONE. I will take that first and then follow up by GAO. The process of CAPPS II and the ambiguity in the address or the name will not result in that individual then being referred to law enforcement.

In other words, the debate is that oh, that ambiguity then may result in me having to go through secondary screening, much like a random selection would be.

Ms. NORTON. Well, at least you do not call the law on me, which really makes the liability question very real, until, perhaps I am on the watch list.

Admiral STONE. If you were one of this very small group of individuals that were matched against a known terrorist list and referred to law enforcement, that would be the issue. But the ambiguity in your address would just result in a score that may make you a selectee for secondary screening and not impact whatsoever your making your flight.

The point which is misunderstood about CAPPS II is this 300,000 folks that we are looking at today that are delayed having to go through secondary screening, we are stating that CAPPS II will dramatically reduce that so that those individuals will get to the gate quicker and help us process people through.

So, in fact, there is a benefit, a goodness to CAPPS II of not hassling individuals who we are currently doing under protocols that we are not fully satisfied with in CAPPS I and facilitate that flow

out to catch your flight and get you on your way, not to make it more difficult.

Ms. NORTON. Assuming we could ever get all the accurate data, would both of you deal with the liability issue for me, please?

Admiral STONE. On the hypothetical of what would happen if under CAPPS II a person was referred to law enforcement and then found that they misinformed them and that there was a law suit involved in that, I would like to get you a more profound answer through counsel on what would be that particular case and what the facts were rather than give a sweeping statement on how that particular individual case would be handled.

But I wanted to echo that web that CAPPS II, the instances of inconvenience which we are currently finding where your people are being delayed while we check the no-fly list and potentially missing flights and being held, this is a reduction in that because of the verification.

Ms. NORTON. Timeliness is going to be everything. What do you think about that question and certainly about liability, Mr. Rabkin?

Mr. RABKIN. In terms of timeliness of the passenger getting through the screening, if the passenger is sent to secondary screening, it may take a little longer.

It really depends on the resource allocation decisions that TSA makes and how many people they have and how much technology they have there to handle that, which in turn depends on their projections of how many people are going to be sent there so they can balance these needs, which, of course, depends on a lot of the assumptions and the planning for the system, which we are still waiting to see.

In terms of the liability, I really do not have an answer for that, so I am going to pass on that.

Ms. NORTON. Admiral Stone, may I suggest that this program is going nowhere until you get an opinion on liability and the notion of saying, hey, there is no liability and asking Congress to say there is no liability. I also think that is a non-starter.

You have to deal with what happens to people who in fact in any imperfect system will be misidentified and will have major losses as a result.

Thank you very much, Mr. Chairman.

Mr. MICA. Well, I think we are going to have to recess here. There are three votes, if members have not heard the announcement. What we will do, I am going to have to ask you to stay. It will probably take us about 20 or 25 minutes to complete those votes.

We will start ten minutes after the last vote has started. We will try to wind it up pretty quickly afterwards.

There may be other members with questions, so we will stand in recess until that time. Thank you.

[Recess.]

Mr. MICA. I would like to call the subcommittee back to order. I apologize to our witnesses. It was a little bit longer than we expected. Sometimes we get into these extensions of time on the Floor and that occurred.

We appreciate your being with us. We may have a few more questions from members as they return. We will see. I do want to state that since we had been interrupted, we will be submitting a series of questions to the witnesses for their response.

Let me check with Mr. DeFazio at this time and see if he has any questions.

Mr. DEFAZIO. Thank you, Mr. Chairman. Mr. Chairman, this is a relatively new issue; well, not a new issue, but a new approach. I mean one of the mandates, Admiral, as you know, of the original legislation was that we not only screen all the passengers, flight attendants, pilots, and in my opinion, all the people who have access to the terminal. I visited that earlier.

But also, we are supposed to be providing screening on the air side. At many airports that is not happening.

I just have seen a story that at JFK they are going to begin implementing a system for air side employees which sounds kind of like a breakthrough. It involves a portal, which I think I mentioned earlier in terms of screening passengers.

I know I have asked some of your colleagues or predecessors about that and they keep raising the privacy concern. I keep telling them that the industry tells me they can put up any figure you want.

It does not have to be your body that they are seeing. The idea is to find whatever contraband you are carrying like a suicide belt, which I think is a very real threat.

But apparently, they are going to implement this portal system for workers out there. Are you familiar with what they are proposing and/or doing at JFK? Do you think it has potential applicability to other airports?

Admiral STONE. I am familiar from the descriptions that I have read of it, sort of a general overview of that concept. I am very familiar with the issue of physical security at our Nation's airports.

Our approach to date has been to place heavy emphasis on background checks rather than in a guns, gates and guards approach.

I have met with my European counterparts to discuss how they do it in the U.K. and in France and in Mexico to get some comparative examples of the approaches.

I have also met with ACI, EEEA, and other partners on the security effort and discussed this very issue.

Our approach has been on enhanced background checks rather than the approach of physically screening those on the air side. The thought is that there are, within the confines of an airport, ample opportunities to attain, once you have been screened, explosive materials, flammables, and build-your-own devices.

To invest large sums of money on physical screening rather than on enhanced background checks, it is our view that that would be a costly endeavor with not the kind of results that we would expect because of the availability of these materials that are within the natural work environment there.

Mr. DEFAZIO. Well, if you consulted with your colleagues in the U.K., then you found that in fact that they do not believe background checks are adequate; that particularly static background checks are not accurate because someone may have become compromised in some way.

They may have extraordinary gambling debts, may have developed a drug addiction, who knows, whatever. But they do not feel that that is adequate. They do both. They do background checks and they physically screen everybody.

Mr. Mica and I filed through with employees carrying their tool boxes and things and everything in the tool box was checked in addition to the person being physically screened, as we were when we were going in and out of security there.

So, do they agree? Who do you find that agrees with your theory that this is adequate? I know the Brits do not, so who of your other European thinks this is adequate?

I understand, I was just talking to ranking member Oberstar and he tells me at Charles de Gaulle that in fact they have a very, very high level of screening, including biometrics for people who have access to the air side.

The French are doing something at a much more secure level. The British are doing something at a much more secure level. So, who is it in Europe? You said you met with European colleagues who agree with us that the background checks are all you need to do?

Admiral STONE. When I said I met with my colleagues, it was to find out what their procedures are. I have met with them. They have a different approach. When I brief them on our 445 Federalized airports and our approach on background checks, they responded that they have much more of a physical security approach where they have invested in their very small handful of airports in that approach.

When we look at that, TSA assesses what type of approach best fits 445 Federalized airports. It is our view that the enhanced background checks and then the regulatory functions that we have to review airport security plans, much like we did at LAX with inspectors to ensure that those regulatory requirements are met, we view as the best approach for that, rather than putting large sums of money into a program on physical security checks when in fact after those checks are conducted, the argument is that you still have those materials resident right in the very work environment that those employees are in every day.

Mr. DEFAZIO. Well, yes, certain materials, fuel and those sorts of things, but not plastic explosives, not guns, not other sorts of prohibited items. Those are not, I would hope, available inside the secure area of the airport on a daily basis.

So, I am just not certain of this and I am not certain that we anticipated this would be the response and/or the end point for TSA when we wrote this legislation.

OK, describe to me an enhanced background check. How often is the person's background checked?

Admiral STONE. The current system that we have today has the fingerprint and the criminal history check conducted. And also we run that against our own lists that we have at TSA for no-fly and selectee.

However, we think a more robust background check is appropriate, to have that conducted through the NCIC with a much more detailed look at that, then being also run against terrorist screening center and our ONRA facility which has databases unrelated

to CAPPS II that we are currently using for international air crews that come and go from our country.

We think that more robust background check of employees at our airports is of greater value to us than the physical security for the reasons that I gave, because of the ability very easily to concoct within the environments of a big airport, whether it is in Charles de Gaulle, and I argued this within my counterparts, to develop within Charles de Gaulle or Heathrow a collecting of these materials such as fuel and other items and building the device then from within.

That was the argument that I proposed with them and they have just chosen a different approach with regard to physical security at eight airports than we have.

I think it is arguable that this intent and the desire to find out about the backgrounds of those that have access is a risk mitigator that is appropriate for that threat.

Mr. DEFAZIO. So, every person who has access on the air side, people who work for the caterer, the cleaners all of those people, every employee of every one of those firms is having this enhanced background check?

Admiral STONE. We have not gone down that road. That is our proposal when asked what would you do today with your background checks that you have at your nation's airports to raise that level.

Mr. DEFAZIO. So, we do not have in place a system of enhanced background checks for people accessing planes on the air side now?

Admiral STONE. No, sir, we do not. That would be our proposal when asked what would you do to enhance the current level of security that you have at our nation's airports for those in the back-door areas.

Mr. DEFAZIO. I guess given the directives from the original legislation, how is it that we have not gone to enhanced background checks?

Admiral STONE. Because it was viewed upon initial review of airport security that the airport security plans that are tailored for each individual airport which have in each of them the backbone of background checks where the airport issues that badge was an acceptable level of security based on the known risk.

So, we have evaluated that and when we look towards what would we do to enhance that, our answers, we think, enhanced background checks would be the way to go on that rather than—

Mr. DEFAZIO. OK, but you do not feel we need to enhance it. So, we do not need to enhance air side security. The minimal background checks are adequate?

Admiral STONE. Our proposal from TSA is that when we have looked at that and said we have this level of security at our Nation's airports, what would you do to improve it, we would propose enhanced background checks.

Mr. DEFAZIO. Right. Do you, in your opinion, think we need to improve it? Do you believe that we need a higher level of security on the air side and if so, when are you going to propose that?

Admiral STONE. Right now I am working on that within the department, enhanced background checks at our nation's airports as

a risk mitigator to reduce the potential threats within the airport itself.

Mr. DEFAZIO. Admiral, I think if the flying public that is standing patiently in very long lines and saying, I understand why I am standing in a long line, I want to be safe when I fly, I think if they knew that at some unknown number of airports, unknown people who work for airport vendors are filing past, carrying bags, suitcases, you know, whatever, large coats, with no security; that mechanics, cleaners, people who work for catering companies who come and go with great frequency are accessing the airplanes with no security and without even the enhanced background checks, I don't think that they would feel real secure and I do not think that they would be very happy that they are standing in line for an hour.

Why are they the suspects? Because there was one operating pattern once where it was the passengers as opposed to employees. These people are smart enough not to try and repeat the same thing and maybe come at it another way.

Plus, there is still a mystery of how did some of those sheetrock knives get on planes, et cetera, which seemed to have come on from ground crews of some sort, cleaners, caterers, whatever.

Yet, you do not feel it is necessary to even go to enhanced background checks on those people. I realize that there is a cost involved. But it is a cost that is dwarfed by the potential for one incident and the loss of one plane and the loss of those lives. I cannot believe that you are not moving forward.

In Europe we have enhanced background checks and physical security and here in the United States we have minimal background checks and no security and we are the people whose planes were hijacked and used as weapons. Now what sense does that make?

I mean no offense, but I mean to say if we needed higher security, we might do this, what are the orange alerts about and what is all this stuff about airplanes and diverting airplanes? We are just focused on the passengers.

Well, you have to get something to the passengers if they are going to take over the plane or maybe it is not going to be the passengers this time. Maybe it is going to be a bomb smuggled on board.

I just do not find that acceptable. I really have to tell you I do not. It is just extraordinary to me that this long after that fateful day and more than two years after we passed the legislation that this is where we are at.

At least to this member in the minority this is not acceptable. I don't believe that were this widely known to the traveling public that they would find it acceptable.

They also might say, well, why the heck am I standing in this line for an hour and a half and having them confiscate tweezers and things from me when these other people are filing through and could be carrying guns, bombs, when we have no technology to detect suicide belts or explosives in briefcases when cleaners and other vendors have free access to the airplane and nobody is checking the stuff they are carrying on.

I am just totally bemused by this, and alarmed, to tell the truth. I am not at all satisfied, but I will apologize for the members who

did not come back because I had a number of members tell me that they wanted the panel to remain because they did have questions.

I do want to at least apologize for having kept you all here and them not having come back. Maybe there are some on the Republican side.

Mr. MICA. We have some members who have returned. Let me recognize Mr. Shuster from Pennsylvania and then we will go down the line here.

Mr. SHUSTER. Thank you, Mr. Chairman. Thank you for being here today, Admiral. I have a couple of questions. First on the CAPPS II system, originally, I believe, TSA said they were going to put a system in place that would pull data through the reservation system of the airlines. Has that changed? Because I am hearing that they are talking about now pushing it through.

My understanding is that it is very expensive and you get less reliability on the information when the airlines are pushing it to you, versus TSA setting up a system that pulls the data through.

Can you comment on that?

Admiral STONE. Our initial intent is to have the airlines, during the testing phase, push that to us and then as we develop the test and see how that works, I am aware that the airlines would like to discuss with us alternative means of providing that data for the operational phase.

Mr. SHUSTER. Does not it make more sense to pull it through because then it will be a uniform system and everybody is going to be providing the information that you want and in the configuration that you want?

Admiral STONE. I will have to get back to you for the record on that on the pros and cons of those different approaches.

Mr. SHUSTER. OK, thank you. The second thing, when you are going to have a rulemaking here compelling the airlines to provide you with that information. Will travel agents also be included in that? Will they have to provide you with the names and different pieces of information from the passengers?

Admiral STONE. That has not been determined. In my discussions with ATA and others they have been a proponent of that approach. We have said we would study that and make sure that that is duly considered as we look at the testing phase and then also the operational phase.

Mr. SHUSTER. It seems to me to make some sense. About 60 or 70 percent of the reservations that are booked are through travel agents.

Mr. DEFAZIO. Would the gentlemen yield for just a second?

Mr. SHUSTER. Yes, I would.

Mr. DEFAZIO. I would hope that you do not just go to the ATA. The ATA represents the airlines. The airlines and the travel agents do not necessarily have the warmest relationship, having been deprived of virtually any capability of making a good livelihood by the airlines.

I have been told by the travel agents and their representatives that there has been no direct contact or any consultation with them and they still do a preponderant amount of the reservations.

I thank the gentleman.

Mr. SHUSTER. And I would urge you also to ask passengers if they are willing to have background checks and pay a fee to do that. My conversation with many, many business travelers said they would be willing to pay that fee to help speed them through the airport, take off some of the burden and reduce those lines.

What status is the Registered Traveler program in at this point?

Admiral STONE. TSA believes firmly in proceeding down the road of Registered Traveler. We anticipate beginning a pilot in June of this year. Airports under consideration are Boston Logan, Reagan National, Dallas Love, Knoxville and Palm Beach International.

We have airlines, United Airlines, U.S. Airways, Southwest, Northwest Delta and American that are interested in partnering with it. This will be a voluntary program and we are looking to focus on groups also that we think will help us address some other risk areas at our nation's airports and also facilitate their entry into the sterile areas.

This includes Leos and Fades and other military personnel, but also the target population will be one in which we are interested in getting at frequent travelers so that we can understand what their needs are.

A key piece of this is going to be the biometric. We think it is critical that RT have a biometric in it so that when combined with CAPPS II you will not only have the benefit of the increased verification of ID which CAPPS II will have a significant jump in terms of the reduction of ambiguity in ID, when you combine it then with a biometric, it is at the point there to address those areas of identity theft and other things that are on our list.

So, this program of combining a biometric and ensuring that we have a full commitment to Registered Traveler this summer is a high priority for us and one that we are eager to move on with.

Mr. SHUSTER. That is very good to hear, that we are moving forward. I know that you are new to this assignment, but it is something I had hoped we would have seen a year ago or sooner. What do you anticipate the testing phase will take before we can have a full-blown program?

Admiral STONE. Our plan is the June commencement with a 90-day pilot and then reporting those results out.

Mr. SHUSTER. That is great to hear. I think that is something that would really help our airports and our airlines in shortening these lines that we see, especially coming into the travel season.

Thank you very much.

Mr. MICA. I thank the gentlemen.

Let me recognize Mr. Ney.

Mr. NEY. Thank you, Mr. Chairman. I apologize. I came in a little bit late, but following up with the gentleman from Oregon's question, right now, as I understand it, like the airports I travel, there are hundreds of people that go through zero screening device that work inside the airports.

If I can follow that up, if that is the case, do we ever intend to screen them? I mean why do anything if—and this is not to also degrade anybody, but some of the people that are going through are making low wages and it would be easier to pay somebody \$10,000 to carry a gun through instead of trying to pay somebody \$100,000. It could be a tempting factor.

Admiral STONE. The best reflective example I can give is take an airport like LAX where you have 60 million passengers a year. So, I got to see first-hand when I was out there, what is the airport security plan, what is my inventory of inspectors to inspect that?

We had programs where Operation Tarmac came through and there were 30,000 badged employees in LAX and only 30 individuals were found for that.

When you look at that percentage, it gives you a high confidence in the credibility of the badging program. It does not mean that it is perfect; that it is the silver bullet we are looking for. But there is a validity to the background checks at that airport and at the other airports that we have across our nation.

It's not perfect, but when you combine those background checks with an aggressive enforcement of airport security plans, I believe that provides acceptable risk.

It is not due to luck that LAX, which is in my mind probably the highest threat airport in this country because of the fact that it was visited at the time of the millennium. The reason why there has not been an attack there, I believe, is because of the deterrent effect of having a very aggressive airport security plan and then regulating that an inspecting it.

Mr. NEY. But they still do not go through a detector.,

Admiral STONE. No, sir, they do not.

Mr. NEY. I am not going to go into details, but here in the Capitol we have changed a lot of things over the last couple of years because you can background all you want, but if they do not go through a detector, you know, it causes a horrific problem.

Let me get to CAPPs II. I do not want to eat up all my time. Let me ask you a question. Information is poured in from different agencies, as I understand this. Let us say an individual, would they look at their passport information or visas to places they have gone to?

Admiral STONE. Right now we are working with CVP on the international flight aspect of that because in fact they have had the responsibility for ensuring that the review of the passports and the checking of those individuals is done prior to entry and departure from this country.

Mr. NEY. I am talking about domestic travel.

Admiral STONE. Oh, for our domestic?

Mr. NEY. Information, yes.

Admiral STONE. For us traveling—

Mr. NEY. Not if you are traveling domestically, but information is poured into this databank and then they type in a name. Somebody is traveling from, you know, D.C. to L.A. They type in their name. Would it show that they have had visas recently to certain countries?

Admiral STONE. No. The concept of CAPPs II is that as a minimum you provide your name, home address, phone number and date of birth. Those four pieces are required. Then if you have additional passenger name record information, P&R data where you have included your VISA card or whatever it is that you have decided to provide, which is currently provided today in that passenger name record, that is the information that will be used to

then pulse the commercial databases in order to get verification of ID, to find out whether there is ambiguity there.

Then that is run against the government databases, the ones that I referred to earlier, the terrorist screening center, to see if that is a known terrorist. So, that would be the process by which that would be followed.

Mr. NEY. I want to go back to the point that was made earlier about that because let's say it is John Smith, perfect record; he has not had anything stolen, has not had a credit card taken and it is John Smith, you know, John Doe Street in St. Clairesville, Ohio. I know about John Smith, so I create a fake driver's license that says John Smith, St. Clairesville, Ohio, and I create that.

I call in my ticket. I give the information and I walk down to a person who is standing there and like I would, flying back from Reagan today, and I hand them an ID and they say well, that is John Smith. John Smith checked out, because I don't know that is John Smith because they do not check the IDs for fraud.

Admiral STONE. That's right.

Mr. NEY. So, I don't know why we are messing with all this. Why do not we just go to an iris scan or facial identification point?

Admiral STONE. I think it is important that we have a way in which we can identify who the individuals are today and run it against a known terrorist list. We need that.

Mr. NEY. But the terrorist is not going to say, oh, this is whoever. Gee, you know, my name is not going to be on it. They are not going to do that. They are going to give you a fake name. They are going to produce an ID and go down to somebody that is standing there at the gate or at the entry point that does not have any way to scan that ID.

They just say, oh, that is your face. A terrorist is not going to put their name down. So, to me, you know, I think the security you are doing at TSA is good. People are searched. But I am just not sure this is going to do anything, anything at all.

Admiral STONE. I think, number one, it is going to significantly enhance our ability to detect known terrorists if they are flying on aircraft by this verification of ID and matching.

Additionally, right now when you have this ambiguity in your identification, CAPPS I does not have that person referred to secondary screening. CAPPS II will. That ambiguity will result in their being given additional opportunity to screen that individual.

You are not going to apprehend them as a known terrorist, but it is that ability to factor in additional risk and then respond to that with additional screening that we think is a significant enhancement.

Right now we are doing it to almost 300,000 travelers a day, with the wrong people in many cases, obviously, that we are looking at.

Mr. NEY. So for the 400 that go through Pittsburgh Airport that could have a gun?

Admiral STONE. Those people are not accessing aircraft though. They are not going on board that flight .

Mr. NEY. I can meet him at the restaurant and I can get the gun from him and walk on that plane. I travel out of Pittsburgh. I can give somebody \$10,000, that's a lot of money, \$20,000, \$30,000.

They go through. They go to a restaurant. I go meet them. I take the gun and I walk right to the plane.

I mean everybody in the country knows this. I don't like to tell secrets. I wouldn't say security I oversee here in the Capitol, but I will tell you this: The whole country knows that. I don't know, nothing is perfect. Neither is our system here.

But there are huge loopholes I think you can drive several Mack trucks through in what we are doing. But I will still argue with you that you can have the database and it is good to check databases.

But that fake ID can be created like that and that person at the gate just looks at the ID. It is your face. It does not have to be identity theft. They just target somebody. I think that is where the failure of the system is.

I am not questions about databases as much as the end result. There is nothing to verify that that is actually in the picture unless you do an iris scan or a facial identity.

Admiral STONE. Sir, I think that the issue of each one of these layers of having a CAPPs II system and then having hardened cockpit doors and FAMs and FFDOs address the various gaps that are mentioned that may exist in each one of those programs. It is the cumulative effect of those layers that we think mitigates the risk.

Mr. HAYES [ASSUMING CHAIR]. Admiral Stone, good day. As Representative Norton said, I'm glad to see you two days in a row. Has TSA conducted a cost-benefit analysis to determine what the airlines have to spent to upgrade their program to meet what you are anticipating?

Admiral STONE. I do not have the data, but I would like to submit that for the record of what the airlines are currently expending and what the forecast costs are for that because we believe it shows the tremendous advantage of us taking over that system and relieving the airlines of it.

Mr. HAYES. Will CAPPs II operate outside of the country and if so, how will you handle the red passengers?

Admiral STONE. We intend on being able to reach cooperative agreements with our international partners on passing that information to their law enforcement so that they can take appropriate measures to mitigate that risk under their own laws and authorities.

Mr. HAYES. Thank you. Mr. Rabkin, in your opinion, do you think that they can deliver a CAPPs II program completed in a reasonable amount of time?

Mr. RABKIN. Well, it is a good question as to what is reasonable. I would call on TSA to better define that, to provide some estimate of a schedule that assuming that they get airline data to test the system in a reasonable amount of time of whatever time they predict for that, how long it would take them to develop policies and procedures to actually implement the program.

Mr. HAYES. Thank you. A resolution would have, among other things to do with Congressman Shuster's question about whether fully appreciated data will be accomplished.

Another question, Mr. Rabkin, do you think that it can be delivered, CAPPs II, as it is described? Do you think it is going to have to be pared back to make it workable?

Mr. POWNER. I will take that. Clearly, it has already been pared back a bit, the initial operating capability. Not only are the schedules being pushed up, but the functionality is being reduced.

That's one of the questions we have in the recommendation in our report where we want to clearly see the functionality defined through initial operating capability and also in those future builds as we achieve full operating capability.

Right now that is unclear, exactly what functionality is to be delivered when and at what cost.

Mr. HAYES. A follow-up question: What level of confidence do you have that the government security bases that are at the heart of the system can be successfully integrated and can function without generating an unacceptable level of false positive?

Mr. POWNER. The confidence we have in the ability to integrate government databases really resides in the ability of TSA and their contractors to effectively test those interfaces associated with those government databases.

For us to predict, it is really not appropriate. We would want to see the facts based on the results of the integration tests with those various databases.

Mr. HAYES. Mr. Rabkin, one more question. A recent GAO report about CAPPs II and privacy-related issues, the report said those issues are not resolved yet. Are you confident that TSA can resolve those issues?

Mr. RABKIN. I think that TSA ought to be able to develop policies and procedures about how they will handle questions of privacy. That can be done independently of the testing of the data that they get.

We haven't seen those policies and procedures, but we think that they ought to be able to develop that, yes, sir.

Mr. HAYES. Thank you. Counsel just reminded me that Chairman Young has this room reserved for 1:30.

Mr. DeFazio?

Mr. DEFAZIO. Thank you. I will move along quickly, Mr. Chairman. Just a couple more points and a question, Admiral Stone.

Admiral STONE. Sure.

Mr. DEFAZIO. One of my colleagues is introducing a bill. It is something that I have been mentioning to all your predecessors and formally to the FAA and others, which is if we are still focused on passengers and we are diverting flights and all that, a key vulnerability on those flights is the fact that the pilot, unlike El Al, where they are sealed in a self-contained unit, have to come out to use the lavatory and/or chat, which I have noticed them doing more of again recently, and have a cup of coffee and/or get food brought into them.

You know, United showed me more than a year ago a very, very inexpensive device which would not require taking a plane out of service. It could be installed overnight. It is essentially a mesh door and weighs virtually nothing. It stretches across, blocking the cockpit area. Now, it certainly wouldn't keep a determined group of people out for as long as a reinforced cockpit door, but it would cer-

tainly give a pilot adequate time to get out of the lav and get back up front behind that door when someone started attacking that.

I would really like to see the TSA move ahead with such a requirement. It is very minimal and I would certainly be willing to work with my colleagues here to look for reimbursement as we did on the cockpit doors because it is just absurd.

Hijackers are not going to be stopped by that, especially since they haven't gotten the training that some of them expected to get. But beyond that, just back to this other issue that Chairman Ney raised and I raised and others have raised about people who work in the airport.

At LAX, a person who works at LAX, who is working, let's not pick on a corporation that exists, at Big Burger, they theoretically have a background check by Big Burger. Big Burger does it or the airport does it?

Admiral STONE. The airport does that.

Mr. HAYES. OK, so the airport does a background check and then that person gets issued an ID card, right?

Admiral STONE. Yes, sir, a badge that allows them access.

Mr. HAYES. And the badge allows them to go around security?

Admiral STONE. Well, at each airport, as you pointed out. At LAX the airport security plan was written that if you are going to Big Burger you have your rotations of your employees during non-peak hours and go through our checkpoints.

Mr. DEFAZIO. OK.

Admiral STONE. So, that is an additional risk mitigator that is in the airport security plan for that airport.

Mr. DEFAZIO. OK, then why wouldn't we want to have that risk mitigator at other airports?

Admiral STONE. Right now you have asked for this list of how each airport—

Mr. DEFAZIO. Right.

Admiral STONE. That currently is what TSA is doing, is going into each of those airports to find out what is unique about the construction of your airport, your checkpoints. Since each airport is so different and diverse, that precludes you from having that policy in effect at your airport.

It is also the study of the Boeing model or what are the economic impacts if we were to mandate that in terms of construction costs at an airport? What does that do to the vendors that are in that area because that complexity is part of that issue, but our intent would be if we could have as a risk mitigator that you go through the checkpoint. That gives us that additional layer.

Mr. DEFAZIO. I mean even TSA employees have to go through their checkpoints, right?

Admiral STONE. That's correct, sir.

Mr. DEFAZIO. So, these people, we know who they are, they are Federal employees. They have been thoroughly vetted. Yet we feel that they are a potential risk. When they come to work they have to go through, a pilot who has had any number of background checks and psychological exams and everything else by the airport and has a history has to go through.

So, I think you are getting my point here. I guess the other question would be are these badges at LAX very sophisticated, non-

counterfeitable, a badge that couldn't in any way be modified and couldn't get a different picture in it or something?

Admiral STONE. No, sir. That's why I think we are eager to go to the TWIC, the Transportation Worker Identification Credential where we can have that biometric.

Mr. DEFAZIO. Thank you.

Mr. HAYES. I thank the gentlemen for his questions. I thank the panel. We will excuse you and ask the other panel to please come forward.

Admiral STONE. Thank you, sir.

TESTIMONY OF JAMES C. MAY, PRESIDENT AND CHIEF EXECUTIVE OFFICER OF THE AIR TRANSPORT ASSOCIATION OF AMERICA, INC.; KEVIN MITCHELL, CHAIRMAN, BUSINESS TRAVEL COALITION; PAUL ROSENZWEIG, THE HERITAGE FOUNDATION, SENIOR LEGAL RESEARCH FELLOW; DAVID SOBEL, GENERAL COUNSEL, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. HAYES. I would like to welcome our second panel to this hearing and introduce Mr. James May, president and chief executive officer of the Air Transport Association; Mr. Kevin Mitchell, chairman Business Travel Coalition; Mr. Paul Rosenzweig, of the Heritage Foundation, Senior Legal Research Fellow; and Mr. David Sobel, general counsel, Electronic Privacy Information Center.

With your permission, we will start with Mr. May. Do you have a comment at this time, Mr. DeFazio?

Mr. DEFAZIO. No. I mean with the next panel we will just move right along.

Mr. HAYES. All right. Thank you. Mr. May.

Mr. MAY. Thank you, Mr. Chairman. I will be brief. I know that time is precious this afternoon.

The Air Transport Association continues to express support for the concept of the Computer-Assisted Passenger Prescreening System, CAPPS II.

As described by the Transportation Security Administration, the goals of this system would be to enhance security and result in fewer hassles and delays for airline passengers.

The safety and security of airline passengers and crews continues to be our top priority and we applaud government efforts to bring a more sophisticated, intelligence capability to aviation security.

Today, billions of dollars have been invested in an aviation system that relies on a rudimentary mix of physical and random screening.

We believe TSA can do better by developing security systems that scrutinize people, not things.

The TSA needs, however, to avoid the dragnet that today captures business travelers flying on multiple one-way tickets or an 83-year grandmother who is unable to even remove her shoes at the security checkpoint.

In the future CAPPS II should improve passenger prescreening by using smart computer systems to identify people who may pose a threat.

U.S. airlines believe there are several operational and privacy issues that need to be addressed.

In short, we believe CAPPS II needs to meet three basic tests. First, we must improve airline security; then it must protect the privacy rights of all airline passengers; and finally, it must be implemented without substantial disruptions to airline travelers or to the public.

Acceptance of CAPPS II will depend on public confidence about the legitimacy of the security system, both here and abroad. Fortunately, Congress and GAO have created several privacy and operational benchmarks for TSA to achieve before CAPPS II is implemented. I stress, before CAPPS II is implemented.

However, it is clear that to improve aviation security, CAPPS I does need to be replaced.

Now, allow me to talk about a couple of the operational highlights. We believe the scope of CAPPS II needs to be narrowed and in fact limited to identifying terrorist or hijack threats. This should not be a program for general law enforcement purposes.

All airline and third-party computer systems are going to have to be reprogrammed to work with CAPPS II. This is going to create substantial new resource demands on our carriers and very little coordination has occurred on that point, if any at all.

U.S. airlines need to know all of the technical requirements for the CAPPS II system, well in advance of the setup, such as how TSA will extract traveler information from airline reservation systems. It is the push-pull question that we talked about a moment ago.

Now airlines do not control how third-party sellers interact with travelers. Since more than 70 percent of all passengers book their travel through third parties such as travel agents and online services, any CAPPS II rules should also require those travel industry partners to collect the required passenger data information. Otherwise, you are going to have 70 percent of your passengers show up at an airport and we have no way of knowing whether that information has been collected or not.

Privacy concerns. Our written testimony reviews in some detail the laws and other requirements to protect traveler privacy and we applaud those efforts.

ATA member airlines remain committed to protecting the privacy of the traveling public as well as ensuring the security of airline passengers. However, CAPPS II clearly raises several privacy concerns for travelers that need to be addressed.

The good news is that Congress has shared these concerns and TSA has acknowledged there is substantial work to do.

Our members know that if the public is not comfortable with TSA's handling and protection of confidential information CAPPS II may well be doomed.

For these reasons, we have developed a statement of privacy principles for TSA to adopt as part of the CAPPS II program. A copy has been provided to each member of the committee and our privacy principles seek to control who is allowed access to passenger information, how that information gets used for identity verification as well as other rules for openness, disclosure and accuracy.

These industry recommendations were approved by the ATA board and are intended for the government to implement consistent with the privacy requirements imposed by Congress.

Two last thoughts: In addition to CAPPs II, we support the Registered Traveler Program. ATA first suggested this program immediately after 9/11 and we continue to believe it should be deployed. In fact it may well make a good test bed for CAPPs II.

International considerations: Obviously, data privacy issues are an important international component of CAPPs II. U.S. and European officials have in fact met. We certainly hope they can agree on data protection principles avoiding conflicts that could easily disrupt travel and create compliance difficulties.

In summary, Mr. Chairman, we believe that the concept of CAPPs II can advance counterterrorism efforts. However, public acceptance of this program will depend on TSA's embraces protections of personal privacy as well as improving the public's understanding of these safeguards.

We also believe there are numerous operational issues that must be addressed before CAPPs II can be launched successfully.

Thank you.

Mr. HAYES. I thank the gentleman for his testimony. Anything that you are not able to include in your testimony will certainly be included in the record.

Now I call on Mr. Kevin Mitchell, Chairman of the Business Travel Coalition. Mr. Mitchell, thank you and welcome.

Mr. MITCHELL. Thank you, Mr. Chairman, and members of the committee. I will substantially truncate my verbal remarks.

There may be rationale for revamping the current prescreening system that BTC and other parties could support, however, we do not yet know what CAPPs II would surely be.

That is to say, we do not understand the privacy and civil liberty tradeoffs required in return for expectations of greater security; nor do we know about the safeguards, remedies, costs, future program growth, or importantly, alternatives to a CAPPs II that might be out there.

Our concerns are explored in much more detail in our written statement, but they fall into three categories: process, product and protections.

First, process. A program with such a far-reaching set of consequences requires very thorough debate based upon an understanding of the projected total costs of such a program over a multi-year time horizon. Knowing the required resources of money, expertise and time would assist both TSA and the industry in evaluating alternative uses of these resources in other programmatic areas of aviation, such as air side enhanced background checks and air cargo.

Second, product. Business travelers are willing to give up some privacy for security if it can be proven that they would truly be more secure. The burden of proof, however, should be on the government. Identity theft is just one issue.

Another example of concern is that a U.S.-based terrorist sleeper cell could throw 50 recruits at a CAPPs II until it identified ten that were color-coded green. Once a person is color-coded green, it

follows that he would be always categorized as such until something fundamental changes in that person's profile

Such a system could provide a false sense of security at considerable cost and actually reduce our absolutely level of security.

Timothy McVeigh, John Allen Mohammed, the Unabomber had no links to terrorist groups. So, what we may be setting up is a Maginot Line where the terrorists just drive right around our fortifications?

Third, protections. Specifically, how would a passenger challenge his risk assessment score and how long would it take to correct inaccuracies in a profile? It is worrisome to business travelers that erroneous information in notoriously unreliable commercial databases might result in their being perpetually flagged for extra screening.

I would like to conclude with just two of the several recommendations in our written statement. One, CAPPS II should be strictly authorized for use only in aviation system security. Adaptations of CAPPS II should not be authorized by Congress for use at interstate toll booths, train stations, sporting events, political rallies or other venues where our freedoms are celebrated.

Secondly, the process and timeframe for both U.S. citizens and foreigners to have their risk profiles corrected needs to be iron-clad and sufficient to a fault. Business travelers currently have claims before TSA for damaged luggage that are 18 months old and still unresolved.

If TSA cannot do right by passengers with such a simple issue, how are business travelers to have confidence that they would have better results with correcting inaccuracies in their risk profiles?

Thank you, with three minutes to go.

Mr. MICA [RESUMING CHAIR]. Thank you for your testimony.

Let me introduce our next witness which is Paul Rosenzweig. He is a senior Legal Research Fellow with the Heritage Foundation.

Welcome, sir. You are recognized.

Mr. ROSENZWEIG. Thank you very much, Mr. Chairman. It is a great pleasure to be back here in this room where I served on the staff so many years ago.

Let me just tell you a story. I was traveling with a Federal judge sometime ago out west at a very small airport that was absolutely no risk of terrorist infiltration. And she was selected randomly for secondary screening, which resulted in her entire bag being emptied and her dirty lingerie being displayed to all of her traveling companions, which mortified her terribly as she hastened us along and said, wait, I will catch up with you because we were waiting to go to lunch with her.

There are two things to learn from that story. The first is that I have no doubt that at that moment she would have traded a little bit of electronic privacy for the physical privacy that was invaded.

I am not so sure that we should so highly value electronic privacy that we do not recognize the other value of physical privacy that we have given up and what that physical security will impose upon us extensively throughout.

Those who would oppose CAPPS II in all of its forms are essentially making the argument that electronic privacy is a higher

value that must be protected absolutely, even at the cost of physical privacy.

To my mind, something like for example Trusted Traveler where one can choose the invasion of electronic privacy or, if one wishes to forego it, accept the heightened physical screening, is the way to go.

But clearly CAPPs II might very well fit a middle ground there. You could perhaps sign out of CAPPs II if you wanted, if you were willing to accept a complete screen of your bags every time you went through.

The other thing, though, that is really notable about this story is that it was an absolute waste. It was a waste of time and money, which, you know, we waste all the time. But it was more importantly a waste of resources that would be much better directed and fixed on combating actual terrorist threats.

This Federal judge was no threat; right? This airport was generically no threat. What is vital to understand about CAPPs II is in however form it ultimately comes about and I certainly agree with many of the criticisms about the need for redress and certainly some of the issues about identity theft, what is vital to understand is that this is not about individual screening per se. It is about risk management and risk assessment.

That means that if it is successful and there is every reason to think that it will be; those who say that it has no hope ignore, in my judgment, its proven effectiveness in the commercial world.

The people in Las Vegas, for example, do this every day to try and screen out, by identifying those who have stolen money from them in the past that they do not want again.

But the proven effectiveness of this will be in allowing us to allocate our resources in a way that targets the limited resources at the true risks, not at the Federal judge or somebody who has passed a top-secret clearance.

One of the things I guess I would leave you with as a last thought is that the risk assessment aspects of this can actually be, and perhaps you might want to, disassociated from the individual screening.

CAPPs II or some risk-assessment program of the sort that CAPPs II is intended to be could simply target higher risk flights, higher risk airports based upon factors of who is booking. That would allow us to surge TSA resources to those areas, not just screeners, but air marshals as well.

Right now screeners and air marshals are essentially randomly distributed in the system and that is completely nonsensical. If we can develop any sort of information system that allows us to better target those resources, even if it does not mean individual screening, we will have gone a long way to better improving our ability to stop terror.

I don't think physical screening is the only answer. I think it is part of the answer. But I think as Admiral Stone said, CAPPs II is an additional layer on top of it.

The Congressional review committee that reviewed 9/11 said that one of our flaws was an unwillingness to aggressively pursue new technologies.

I would urge us not to make the same mistake. CAPPs II needs a lot of work, I agree, but do not kill the baby now.

Thank you.

Mr. MICA. Thank you for your testimony.

Our last witness is David Sobel. He is general counsel of the Electronic Privacy Information Center.

Welcome, sir. You are recognized.

Mr. SOBEL. Thank you, Mr. Chairman. I have submitted a written statement for the record.

Mr. MICA. Without objection, the entire statement will be made part of the record. Please proceed.

Mr. SOBEL. Thank you and thank you for the opportunity to address the civil liberties implications of the CAPPs II system now under development within the Transportation Security Administration.

The subcommittee's inquiry is critically important and goes to one of the most significant controversies surrounding the Government's response to the tragic events of September 11th.

While most of the post-9/11 debate over security and liberty understandably has focused on the USA Patriot Act, the serious problems inherent in CAPPs II will have a more direct and immediate impact on most Americans.

The CAPPs II mission to conduct background checks on millions of citizens is unprecedented in our history.

While we all agree that there is a clear need for enhanced aviation security, there are many reasons to question whether CAPPs II is the right approach, both from a security perspective and in terms of the detrimental impact on our traditional liberties.

The Supreme Court has long recognized that citizens enjoy a constitutional right to travel. For that reason, any government initiative such as CAPPs II that conditions the ability to travel upon the surrender of privacy and due process rights requires particular scrutiny.

I hope that today's hearing marks the beginning of a serious inquiry into the costs and claimed benefits of CAPPs II and that there can be an informed public debate on the proposal, a debate that has not yet really occurred.

Critical elements of that discussion which I address more fully in my written statement include transparency, due process, and adherence to established privacy principles.

The problems that are likely to arise if and when CAPPs II is implemented are not hypothetical. For more than two years an untold number of innocent airline passengers have been wrongly flagged as a result of TSA's secretive selectee and no-fly lists.

Documents obtained by my organization under the Freedom of Information Act detailed the Kafkaesque dilemmas that scores of citizens have confronted when they attempt to learn why they are consistently flagged at the airport and when they attempt to clear their names.

TSA refuses to provide these individuals with any explanations and the agency's claimed procedure for addressing these problems has proven to be wholly inadequate.

Although few details of CAPPS II have been disclosed, the Privacy Act notice for the system that TSA published last August provides a basic outline of how it would operate.

In essence, CAPPS II will be a secret, classified system that the agency will use to conduct background checks on tens of millions of airline passengers. The resulting risk assessments will determine whether passengers will be subject to searches of their persons and belongings or be permitted to board aircraft at all.

TSA will not inform the public of the categories of information contained in the system. It will include information that is not relevant or necessary to accomplish its stated purpose of improving aviation security.

Individuals will have no judicially enforceable right to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete.

This is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act in 1974. When it enacted the Privacy Act, Congress sought to restrict the amount of personal information that Federal agencies could collect and, significantly, required agencies to be transparent in their information practices.

Because—and this is a key point—because TSA has exempted CAPPS II from most of the key Privacy Act requirements, secrecy rather than transparency will be the rule.

This problem is exacerbated by the fact that today, more than two years after TSA began development of CAPPS II, the agency has still not published a privacy impact assessment for the system as required by the E-Government Act.

As the recent GAO report found, TSA has failed to adequately address the very real privacy and due process issues that permeate the proposed system.

Based upon TSA's Privacy Act notice for this system, I believe there is reason to doubt whether the system as currently envisioned can ever function in a manner that protects privacy and provides citizens with basic rights of access and redress.

Thank you for your attention. I will be happy to take your questions.

Mr. MICA. I thank you and I thank all of our witnesses, both for their patience and for their testimony. We have been interrupted. I think some of you have been here before and know the process.

I have a few questions and then I will yield to the ranking member and other members.

Mr. May, I think we have one purpose in trying to develop a CAPPS II system that does not intrude on privacy and that does not discriminate and that is to expedite the passage of our passengers of our passengers through commercial aviation.

That is so important because again if we look at the three million jobs that have been lost since 2001, probably half of them have been related to the aviation industry, if not more,

One of the hurdles that you have representing the airlines is that the airlines can be subject to liability giving out certain types of information.

If TSA does pass a rule, and we have given them complete authority to pass rules relating to our needs in this particular era in

which we live, is that sufficient to protect you or are you going to need additional legal coverage to satisfy your members as far as liability?

Mr. MAY. Mr. Chairman, I was pleased to hear the administrator this morning talk about the fact that he, I think, if I heard him correctly, plans on issuing an NPRM as opposed to a security directive. I think, you know, we need to take a look at that NPRM and figure out what the implications are, sit down with counsel and get a feel for it.

I don't think there is any question that we are concerned about our liability. I don't think there is any question that we feel far more secure if they require that information as opposed to us volunteering it.

In fact, I think it would be safe to say the likelihood of us volunteering it in the future is somewhere between zip and zero. And I think that finally there needs to be a privacy policy in place. Everybody is talking about it, but nobody has done it.

Mr. MICA. Well, again, the question is, and you may have to come back with opinions from your legal counsel, with it is a security directive or a rule through the process that has been announced today, what is going to cover you and what would be the quickest remedy and satisfy you.

Can you do that? Can you give us your opinion?

Mr. MAY. I cannot give you the answer I suspect you want today, Mr. Chairman. I will be happy to come back to the committee.

Mr. MICA. Well, I am going to direct a question to you and your counsel to come back to the committee.

We are going to keep the record open by unanimous consent for a period of two weeks. I am hoping that you can come back with us. So, without objection, it is so ordered. The record will be open for that period of time, not only for your response, but for other responses we may be submitting to TSA and other witnesses today.

Mr. SOBEL, if we can meet some of the objections which you have cited today and which Congress has also expressed concerns about, do you think we could develop something that is acceptable from your perspective?

Mr. SOBEL. I think, Mr. Chairman, that TSA would really need to be much more forthcoming about the information that is going to form the basis of this system than they have up until now.

TSA's position seems to be, and it is certainly reflected in the fact that they have designated this system as sensitive and classified, that the effected citizens who are flagged by the system are not going to have full access to the underlying information that has resulted in some type of negative security assessment.

So, it is really a question of whether TSA is ever going to be able to get over that hurdle that it seems to have about opening up this process to real citizen access and a real means of a judicially enforceable right to correct inaccurate information.

That is what the Privacy Act requires. I think the key defect thus far is that TSA does not seem to be willing to comply with those Privacy Act requirements.

Mr. MICA. OK. Thank you. Mr. DeFazio.

Mr. DEFazio. Thank you, Mr. Chairman. Mr. May, have the airlines been working closely with the TSA regarding the parameters

that would be required of the airlines to provide and how that might be done?

Mr. MAY. Mr. DeFazio, I think the best answer to that question is to say that we have had a number of conversations with TSA, with whom we do have a good cooperative relationship, on the subject of CAPPS II to identify for them what we think are numerous operational hurdles that need to be scaled.

I am not sure that we have any real answers and I am not sure that we have a process yet in place to resolve some of those issues that we have identified.

Mr. DEFAZIO. As I understand it from their testimony though, they are looking at four parameters that they would want from the airlines, is that correct? I mean in the database.

Mr. MAY. In terms of the information?

Mr. DEFAZIO. Yes.

Mr. MAY. I don't think there is much question in anyone's mind, quite frankly, as to what the information they are interested in having is. It is full name, home address, home telephone number and date of birth.

Mr. DEFAZIO. Right.

Mr. MAY. But, you know, that is the least of our concerns. We talked a little bit about push and pull. We have a ton of different IT systems that contain information, you know. If the TSA wants to have a single system, come look at what we have, that is one option and it may be the easiest.

What they want to do is have all of these different IT systems push information to them, to a single resource. Well, that means we have got to do significant reprogramming. It is a major hurdle. We understand. I have talked about it.

You know, you suggested we do not have a warm and fuzzy relationship with our travel agent friends. I certainly think they are fine people.

Mr. DEFAZIO. I think they are fine people, too. I think they are under-compensated by the airlines, but that is a different story altogether.

Mr. MAY. That is a different story altogether. I think the very real concern is that if you have 70-plus percent of the reservations being made by someone other than the carriers, then that information has to be collected at the time the reservation is made, if we are going to go forward with this.

Mr. DEFAZIO. Right.

Mr. MAY. And then you have to figure out how that information gets from that travel agent or reservation center, whatever it is, to the TSA. Otherwise, if you are talking just the airlines, you are only going to talk about 20 percent of the flying populous.

Mr. DEFAZIO. Well, I am assuming that the way this would be worked out, I mean you are raising the question of which way it goes between the TSA and the airlines, but the airlines become the repository with the reservation.

So, if a travel agent makes the reservation, they have to communicate that reservation to the airlines and at that point, apparently, they would be required to transmit that information to the airline. So you would become the repository or the airlines would, as far as I can tell.

Mr. MAY. And clearly that raises all sorts of other questions, too.

Mr. DEFAZIO. Right.

Mr. MAY. They are not exactly excited about providing a lot of the fields in P&R to the airlines.

Mr. DEFAZIO. Right.

Mr. MAY. And so I think those are clear operational concerns that we have that have yet to be addressed in a very practical way and must be.

Mr. DEFAZIO. You say, point four, government shall only use collected information for aviation security purposes and shall not use the information for law enforcement purposes not directly related to aviation security.

So, the ATA's position is if the system, when you have provided date of birth, home address, full name and it turns out that that person is a wanted criminal, that the TSA should not be able to contact law enforcement authorities and pick that person up.

Mr. MAY. I don't think that is what we are suggesting in this case, Mr. DeFazio. I think what we are suggesting is that there needs to be some line drawn as to how this information will be used.

It is collected to protect against terrorism, hijacking of airplanes and that is how it should be used. To the extent we can eliminate or minimize the collateral use of that information for pure law enforcement purposes, I think that needs to be done.

Carriers do not want to be in the business of law enforcement.

Mr. DEFAZIO. Right. But the point is, I just think that then perhaps you need to reword that point. I mean if the system should uncover a known felon and that person has a reservation, it may well be, since the law enforcement has been unable to find them, that they would actually want the airline to cooperate; they would want that person to show up for the flight and then they would apprehend them.

In fact, this just happened recently in Portland, Oregon, but it had to do with Customs and some other issues for a fugitive overseas felon.

I think maybe that needs a little rewording there. I understand what you are trying to get at, but I mean this may well turn up law enforcement actions that are needed and we may well want to ask for some cooperation. It is not to create a dragnet. This may cause some concerns over here, but it does not to me.

I mean if someone is a fugitive felon and we find them, that is great as far as I am concerned. But that is not where I am talking about people who have other incidental sorts of things in their background.

Mr. Sobel, when you raised the concerns, for years I have heard concerns and frustrations from my constituents who end up having bad information on their credit report and have to go through extraordinary efforts to correct that.

Then you are raising the issue in part, apparently this may or may not, depending on what parameters you use, rely upon credit reports to rate the risk of these individuals. So we may take that information and pile it into, now, a government system.

The point you are raising is if you had communication with TSA and why is it they say that the person would not be able to review the data which would deny them the capability of flying?

Mr. SOBEL. Well, certainly on the side of the equation where they are looking at government information, presumably information obtained by other agencies, CIA, FBI, whatever it is, they seem to take the position that that information is often going to be classified, derived from intelligence sources.

While that is understandable that there are watch lists that derive from that kind of information, the problem is a situation like we are talking about where the government is starting to make decisions about what citizens can or cannot do without certain hurdles being placed in their way, based on that kind of information and saying to them, sorry, we have a reason but we cannot share it with you.

I just do not see how a system like CAPPS II as currently envisioned can avoid that basic problem. I believe that is the reason why TSA has seen it necessary to exempt this system from many provisions of the Privacy Act.

For instance, the one I pointed out, no judicial review of a citizen request to correct, first of all to access and then to correct any information that might be inaccurate. That is ultimately the way that a system like this is going to have due process built into it.

Admiral Stone, this morning, talked about the fact that there would be an ombudsman within TSA and a passenger advocate. That is all well and good, but unless there is some type of statutory time limit for TSA to make a correction decision and then either if they do not make that deadline or if the determination is against the passenger, the passenger should have a right to go to court and review that decision.

Otherwise, I think these things are just going to languish at TSA, unresolved for months on end. It is going to have a real impact on people's ability to travel.

Mr. DEFAZIO. So, Mr. Rosenzweig, would you share those concerns? I am certain Heritage, having a conservative viewpoint would think that people should have some redress.

Mr. ROSENZWEIG. Absolutely. One of the things I have written about is the need for an adequate redress system. That is one of the aspects of CAPPS II that has not yet been fully planned out, as we heard today.

I think, though, that it is sort of important to understand exactly what Mr. Sobel is at least in theory talking about. If the watch list that we are discussing is a CIA watch list that is developed through covert intelligence means and somebody's name has come up on the list, it is going to have to be something other than full-scale judicial review in a public court to discuss the errors that might be on that list. It has to be.

I mean we recognized that already in the Classified Information Procedures Act. We are going to have to modify or apply graduated transparency. I am in favor of transparency, but it cannot be that—I mean, for one thing I think that the number of misidentified on the watch list red cards is going to be relatively small.

So, as opposed to substantial secondary screening which may be larger, that is where the errors are more likely to occur.

Mr. DEFAZIO. I did not have time to go back again to Admiral Stone, but what do you envision the secondary screen is? Right now under CAPPS I, it just means you get diverted over here and they search your luggage and they search you.

Here are we talking about an interrogation?

Mr. ROSENZWEIG. I think that the interrogation, as I understand the system being built, the interrogation is for the red card. The additional screening is going to be additionally the same form that you or I get right now if we have too much metal on us or as is the case when I sometimes travel, you have made a one-way reservation and you have made the absolutely useless CAPPS I system.

Mr. DEFAZIO. That is right.

Mr. ROSENZWEIG. Yes, then they pull you aside and they go through it. It will be, you know, stick out your arms and legs.

Mr. DEFAZIO. Sure, and they wand your bare feet to make sure there is nothing in there.

Mr. ROSENZWEIG. Yes, they wand your bare feet. It is a waste. It really is a waste of resources. I think everybody agrees that what we have now, except maybe the fellow from GAO, that what we have now is worse than useless because it is costing money and doing nothing.

So, the secondary screening for unverified identity will just be what we have today.

Mr. DEFAZIO. But I think there may be some grounds for agreement here although perhaps Mr. Sobel wouldn't, as you say, want to take it further to find out. But there certainly should be protections on classified information.

But if it is a result of some other public database or any kind of mistaken identity or something like that, that should be absolutely transparent and people should have the right to correct it, like they do not have with their credit bureaus today.

Hopefully, the government can do a better job than the credit bureaus are doing.

With that, Mr. Chairman, thank you.

Mr. MICA. I thank the ranking member. I want to thank our witnesses for being with us today. I understand several had requested additional information of witnesses to be included as part of the record.

Without objection, that is so ordered.

I want to also welcome to the subcommittee students from Orangewood Christian School. We have some 11th graders from Florida who came up to enjoy the cold weather. Welcome to the aviation subcommittee this afternoon.

This is a hearing that has dealt with passenger screening and a new passenger profiling system that is being proposed. This is the second and last panel of witnesses.

We thank you again for your cooperation. We thank the students for their attention, coming in at the end of the hearing here.

There being no further business before the subcommittee—

Mr. DEFAZIO. Well, Mr. Chairman, I just want your students to know you are a very important Member of Congress. You can tell because he gets a bigger chair than everybody else who is sitting up here.

Mr. MICA. Well, I just want the students to understand that we do, believe it or not, we do have a very bipartisan system of government. There is very little that I can do as chairman without the ranking member, Mr. DeFazio.

And so we sort of equally share. I get to chair the hearings, but I think we have a very good working relationship. Most of the issues before us are not partisan issues, Republican or Democratic. They are issues for the welfare of the country.

We do have a great working relationship on those issues. Believe it or not, MR. DeFazio, who comes from the other side of the aisle, and I often agree. Sometimes you see us in concert, like today, on a number of issues, trying to improve safety and security for the American people.

So, that is how the system works. We are graced with two great counsels here who help us.

Mr. DEFAZIO. If we are getting warm and fuzzy, could we talk about staff ratios and how we could use a little more money on our side, Mr. Chairman?

Mr. MICA. Having been in the minority, just a little lesson in political science and government, it is much better to be in the majority.

With that, there being no further business before the aviation subcommittee today, this meeting is adjourned.

[Whereupon, at 1:48 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

**Opening Statement of Congresswoman Shelley Berkley
Subcommittee on Aviation
Hearing on the Status of CAPPS II
March 18, 2004**

Thank you, Mr. Chairman for holding this important hearing. Since September 11th, Congress has made difficult decisions about how to best provide for the security of all Americans. We have passed laws giving law enforcement tools to find terrorists and created programs and agencies tasked with improving our homeland security. Throughout this process, we focused on balancing national security and our civil liberties, and once again, we are faced with that challenge.

The goal of the CAPPS II program is to identify potential terrorist threats and make our aviation system safer. In doing so, the Transportation Security Administration must address privacy concerns and create a system that can accurately identify passengers who should receive additional scrutiny. However, if a passenger is inaccurately identified for additional screening, there must be a procedure in place to quickly review and correct the mistake.

I have very serious concerns about how the information that is collected by the system will be used. As you know, in our desire to create safer communities and prevent terrorism, Congress passed the Patriot Act. However, the Patriot Act has been used not only for combating terrorism, as was intended, but for a political corruption investigation in Las Vegas and for other purposes which fall outside the law's original intent. To prevent this from happening in the future with the CAPPS II system, I believe it is imperative the Transportation Security Administration clearly outlines for the public the specific ways in which the information will be used before the system is ever implemented.

More than 35 million people from all over the world come to Las Vegas each year. While the security of our visitors is a top priority, travelers should not be subjected to overly intrusive procedures that may dissuade them from visiting our community.

This is an important hearing, and I look forward to the testimony from the witnesses.

**Statement by Congressman Jerry F. Costello
Committee on Transportation and Infrastructure
Subcommittee on Aviation
Hearing on the Computer Assisted Passenger Prescreening
System (CAPPS II)
March 17, 2004**

Thank you Mr. Chairman. I'd like to thank you for calling today's hearing as we continue to discuss passenger screening and aviation security.

The Computer Assisted Passenger Prescreening System (CAPPS) was approved in 1998 by the FAA as a system to allow air carriers into two categories: those who are flight risks, needing additional screening, and those who are not. Based on certain factors, an individual's boarding pass will indicate whether the passenger is a flight risk or not, and the passenger will be subject to additional screening measures.

However, CAPPS has been criticized because it is not seen as focusing on people who are indeed the biggest flight risk, but rather those people who have bought a ticket at the last minute, have purchased one-way tickets or have used cash to purchase tickets. Many of us on this committee are familiar with horror stories of our constituents' parents or grandparents who are singled out as security risks because they paid cash for their tickets—but are clearly not security risks.

As a result, the TSA has been working on implementing an improved version of CAPPS, to be known as CAPPS II. CAPPS II will require passengers to provide their full name, home address, home phone number and date of birth when they check in for a flight. This information will be checked against a commercial data base to determine an identity authentication score. Based on this score, CAPPS will conduct a risk assessment using information in a government database. The risk assessment—which is essentially high, unknown or low-- will then be transferred to the check-in counter, and the passenger will be issued a boarding pass (if unknown or low risk) and sent on through security. If the passenger is high risk, law enforcement will be contacted.

While it appears that CAPPS II will focus more directly on passengers who are indeed security risks, there are still flaws in the system as proposed. I am not confident that all of the privacy issues have been resolved and I would like more information on how the system will deal with the issue of identity theft. I am also concerned with issues that the GAO brought up in its recent report and how the TSA is addressing these issues.

I look forward to today's hearing and hearing from today's witnesses.

COMMITTEES:
TRANSPORTATION AND
INFRASTRUCTURE
SUBCOMMITTEES:
AVIATION
HIGHWAYS, TRANSIT & PIPELINES
WATER RESOURCES & ENVIRONMENT

SCIENCE
SUBCOMMITTEES:
RESEARCH, RACING MECHANICS
SPACE & AERONAUTICS
DEMOCRATIC ASSISTANT
WHIP
CONGRESSIONAL BLACK CAUCUS
CHAIR, 107TH CONGRESS



Eddie Bernice Johnson
Congress of the United States
30th District, Texas

SUBCOMMITTEE ON AVIATION
HEARING ON CAPPS II
MARCH 17, 2004 10 A.M.

PLEASE RESPOND TO:
WASHINGTON OFFICE:
1511 LONGWORTH BUILDING
WASHINGTON, DC 20515-4331
(202) 225-8885

DALLAS OFFICE:
CEDAR SPRINGS PLAZA
2501 CEDAR SPRINGS ROAD
SUITE 550
DALLAS, TX 75201
(214) 922-8885

IRVING OFFICE:
1634 B WEST IRVING BOULEVARD
IRVING, TX 75061
(972) 253-8885

www.house.gov/ejohnson/

Thank You Mr. Chairman.

I appreciate you holding this hearing this morning.

The Computer-Assisted Passenger Pre-Screening System (CAPPS II) has the potential to adversely impact our nation's security, economy, and civil liberties, and it's important that we closely monitor the process as CAPPS II develops.

This issue is of particular importance to me for several reasons:

- 1) The economy of the Dallas-Fort Worth area heavily depends on a healthy aviation industry. Providing safety and security to the flying public is crucial to the economic well-being of my constituents and our nation's economy.

- 2) I have heard from my constituents on this issue. They are following this issue closely. They are extremely concerned about what they believe are intrusive background checks. Many of them believe that we are putting money into an untested program that provides little or no additional security.
- 3) Also, let me just say that protecting civil liberties is a part of providing the safety that the American people both expect and deserve.

I know that we are here today to address these issues.

So this morning I'd like to focus on the potential unequal impact that CAPPs II could have on communities of color. The muslim faith is the fastest growing religion in the african-american community.

Many people are changing their names to Muslim names without realizing the implications this could have on their ability to travel without being profiled. I am concerned that CAPPs II could have a disparate impact on African-americans, latinos, and arab-americans.

I hope that TSA has plans to monitor the number of people of particular ethnic groups that are flagged for increased scrutiny. This is vital information that must be collected in order to assess whether the program is profiling particular communities of color. I am interested in hearing about any plans to count those black, latino, and arab travelers that are stopped in relation to white travelers that are stopped.

I welcome our witnesses here today, and I look forward to asking some questions.

Thank You, I yield back.

**STATEMENT OF
JAMES C. MAY
PRESIDENT AND CEO
OF THE
AIR TRANSPORT ASSOCIATION OF AMERICA, INC.
CONCERNING THE STATUS OF THE
COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM ("CAPPS II")
BEFORE THE
AVIATION SUBCOMMITTEE
OF THE
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
OF THE HOUSE OF REPRESENTATIVES
MARCH 17, 2004**

The Air Transport Association has repeatedly expressed support for the development of appropriate measures to improve the Transportation Security Administration's ability to evaluate the security implications of those who present themselves for transportation on air carrier aircraft. More particularly, we have supported the concept of the Computer Assisted Passenger Prescreening System (CAPPS II), which is under development by TSA. Although we are not privy to the details of CAPPS II, it is envisioned to provide markedly more effective passenger screening capabilities for TSA, which should result in fewer security checkpoint delays for passengers. This is a goal that we all share. While the promise of CAPPS II is impressive, many significant issues concerning its nature, implementation, and personal privacy implications remain unresolved. Any final judgment about CAPPS II, therefore, must await resolution of those issues.

Favorable resolution of those issues will require CAPPS II to meet three basic tests. It must be efficacious, implemented economically and protect airline customers' privacy rights. CAPPS II must be *efficacious* in the sense that it appreciably advances

civil aviation security and does so efficiently. CAPPS II must be *implemented economically* in the sense that it places minimal new demands on affected third parties, such as airlines, travel agents, and global distribution systems. CAPPS II must *protect airline customers' privacy rights* because they are entitled to that protection and the public will not accept the program unless those rights are safeguarded.

Acceptance of CAPPS II will largely depend on the government generating public confidence, both in the United States and overseas, in the legitimacy of the System. Importantly, however, public acceptance will also depend on a very practical consideration: avoiding CAPPS II-related delays during the reservation and airport check-in processes. CAPPS II cannot be seen as contributing to the "hassle factor." Achieving these objectives is imperative. If they are not realized, the public could come to regard CAPPS II with suspicion or hostility.

All of us in the commercial aviation community have a stake in this outcome. If the public rejects CAPPS II, the very real risk could emerge that travelers will forgo the use of air transportation.

Fortunately, however, Congress has created benchmarks against which all concerned can evaluate CAPPS II as it proceeds through its developmental stages. Congress in Vision 100 enacted two provisions, sections 607 and 608, which establish important pre-implementation certification and reporting requirements concerning CAPPS II. Public Law No. 108-176, December 12, 2003. Section 607 prohibits the Department of Homeland Security from proceeding beyond the test phase until the Under Secretary for Border and Transportation Security certifies to Congress that CAPPS II has met eight specified developmental, operational and personal privacy requirements. The

General Accounting Office last month submitted a report to Congress about the status of accomplishing those requirements. U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385, February 2004.¹ Section 608 of Vision 100 requires the Secretary of Homeland Security, after consulting with the Attorney General, to submit a report to Congress by March 12th about the potential effect of CAPPS II on the privacy and civil liberties of U.S. citizens.

The February GAO report identified the ongoing challenges to the development of CAPPS II. The report has attracted considerable attention because it described important CAPPS II developmental issues that remain to be completed. Nevertheless, the GAO report and Vision 100's CAPPS II certification and reporting requirements demonstrate that authoritative evaluations of developmental, operational and privacy issues will be undertaken before CAPPS II is implemented. This Congressional-ordered scrutiny should greatly facilitate public confidence in CAPPS II as it ultimately emerges as an operating system.

That public acceptance would be greatly advanced if the scope of CAPPS II were narrowed. The widespread impression is that CAPPS II is intended to assess the security risk that passengers pose and identify those who require additional security attention because of the possibility that they could commit acts of violence aboard a commercial aircraft. In fact, however, the scope of CAPPS II as presently conceived would go beyond identifying potential terrorists or hijackers. It would also include those with

¹ The Department of Homeland Security Appropriations Act, 2004, Pub. Law No. 108-90, §519, 117 Stat. 1137, 1155-56 (2003), instructed GAO to assess CAPPS II's development, including its privacy protections. The Congressional mandate in section 519 of the DHS Appropriations Act is similar to the requirements of section 607 of Vision 100. See GAO report 04-385 at 3 n.4.

outstanding state or Federal arrest warrants for crimes of violence. The desirability of identifying such individuals is beyond dispute but this remains a federal law enforcement responsibility. The problem, however, is that the acceptability of CAPPS II will depend on convincing the public of its unbreachable, tightly focused purpose. Including a surveillance system for a non-terrorist category of individuals could undermine achieving that support.

IMPLEMENTATION CONSIDERATIONS

Implementation and application of CAPPS II will impose substantial new requirements on passengers, airlines and other reservation and distribution entities. Passenger name records do not contain all the categories of information that TSA contemplates will be required for CAPPS II. CAPPS II will consequently require airlines to change significantly their practices for acquiring information from customers.

The essential implications about the anticipated CAPPS II passenger information collection requirements are:

- Airline reservation systems and the reservation systems of global distribution systems and online reservation systems will have to be reprogrammed to respond to the new information collection requirements. This will create substantial new resource demands on airlines and other providers of reservation services.
- Because of the necessary reservation system reprogramming and revision of reservation agent practices to accommodate CAPPS II, airlines will need to know the technical requirements for and implementation schedule of CAPPS II well in advance of its startup. TSA, however, has not yet

provided airlines with specifics about the CAPPS II system architecture and initially suggested that the system would pull the required data elements from computer reservation systems. Representatives from the Office of National Risk Assessment now indicate that reservation systems will be required to push data to TSA's CAPPS II system, which will result in additional programming and operating costs for airlines and other reservation system operators.

- The required CAPPS II information, which must be collected from every passenger, will be more intrusive for the passenger than today.
- Information in many instances will be obtained from passengers orally and entered manually into reservations systems. Reservation call "talk time" will increase markedly, affecting the length of time a consumer is on a reservation call and the cost of such calls to air carriers. This will not only impose greatly expanded resource demands on airlines, it will also place new demands on the time of customers.
- Airlines do not control third parties, such as travel agents and online booking entities, through which the majority of air transportation is purchased. Any failure of such a party to obtain mandated information will have to be remedied at the airport, which will delay passenger processing and inconvenience customers.
- Airlines are concerned about the potential international applicability of CAPPS II. This is a serious consideration which must be addressed because foreign governments presumably would be responsible for

conducting additional screening of selectee passengers if CAPPS II is applied overseas.

One of the foregoing points bears special emphasis: because the majority of reservations are made through third parties, most notably travel agents, airlines often do not have direct contact with the passenger until he or she arrives at the airport. This means that airlines cannot assure that information is collected from such customers at the time of reservation. Any CAPPS II rule must recognize this fundamental characteristic of airline distribution and mandate that third parties collect needed information at the time of their first contact with the customer. The failure to do so will result in serious delays for airline passengers at airport check-in, where airline customer service agents will have to collect from them the information that is necessary for CAPPS II.

The foregoing is not meant to be an exhaustive explanation of the implications of the mandatory collection of CAPPS II passenger information. It is intended, instead, to underscore that changes in the reservation and passenger processing environments will have substantial consequences, including added expenses and the likelihood of increased customer processing times.

PRIVACY CONSIDERATIONS

Customers must be confident about the legitimacy of the government's access to, handling of and disposition of personal information that it will use in evaluating them. Legitimacy in this context intertwines both the issues of the effectiveness of the System's privacy protections and the efficacy of CAPPS II, which we discussed above. Concern about the legitimacy of CAPPS II was evident in public comments reacting to TSA's January 15, 2003 Privacy Act-related notice of proposed rulemaking. 68 Fed. Reg. 2002

(Jan. 15, 2003); *see* Department of Transportation Docket OST-1996-1347, *accessible at* <http://dms.dot.gov>. TSA, to its credit, has responded to the critical public comments that it received about that proposal. TSA in its August 1, 2003 interim final Privacy Act notice clarified its intentions about the application of CAPPs II and modified several of the System's routine uses to respond to concerns expressed in those comments. *See* 68 Fed. Reg. 45265, 45267-68 (Aug. 1, 2003).

Even with the modifications that TSA described in its interim final Privacy Act notice, however, CAPPs II will require airline customers to sacrifice an appreciable amount of privacy if they are to be permitted access to air transportation.

The implication of this is clear. If the public is not comfortable with the various facets of CAPPs II, its acceptance will be imperiled. Were that to occur, air transportation would suffer because some passengers would regard the privacy demands of CAPPs II as personally too costly to justify traveling by air. Thus, the government's development of CAPPs II personal data privacy protections should be thorough and its explanation of those measures should be clear. In addition, it should be made clear who within TSA will have access to the information gathered under the program.

TSA discussed these matters in its interim final Privacy Act notice. We foresee, however, that this will be an important, persistent concern of the public. Indeed, this predictable concern is likely to be more pronounced because of the involvement of commercial entities in the CAPPs II passenger authentication process. Such an explanation from TSA, therefore, would allay the very understandable concern about whether the scope of an authorized individual's access to and use of information will be as limited as practicable and directly tied to her or his aviation security responsibilities.

TSA should also explain what penalties will be imposed for unauthorized access to or misuse of that information.

We also believe that when CAPPS II is implemented the TSA needs to notify the public on its Web site and through other channels of the measures that it has undertaken to assure the privacy of passenger information. TSA is the only authoritative source of such an assurance. Consequently, providing such notices should not be the responsibility of airlines.

REGISTERED TRAVELER PROGRAM

In the aftermath of 9/11, ATA suggested the creation of a “trusted” traveler program. Our view then, and it continues today, is that more should be known of those presenting themselves for air transportation. Greater attention should be paid to who the passenger is, rather than continuing to rely disproportionately on the screening of objects to provide aviation security. For that reason, recent indications from TSA that it is considering a registered traveler program are intriguing. More, however, needs to be known about such a program before it proceeds. In particular, its benefits need to be clearly articulated and who will pay for it needs to be determined; our view is that airlines should not be required to pay for it. These issues should be resolved promptly so that all concerned can determine if this is a viable concept.

INTERNATIONAL CONSIDERATIONS

There is an important international component of the CAPPS II data privacy issues. The Department of Homeland Security and the Department of State have met with European Commission data protection officials to discuss privacy issues associated

with the Bureau of Customs and Border Protection's access to passenger name record data for customers on flights to the United States. Those discussions, which were recently completed, have highlighted European concerns about the adequacy of U.S. data privacy protection practices. European authorities have specifically expressed those same concerns about CAPPS II. We hope that U.S. and EC officials can agree in their future discussions on data protection principles that will be applicable to CAPPS II when it is introduced and thereby eliminate the possibility that U.S. airlines will be caught between conflicting U.S. and EC regulatory requirements.

We believe that public acceptance, both in the United States and overseas, of CAPPS II will depend on the Federal government's assurance of suitable privacy protections and passengers' understanding of them. We also believe that the implementation and operational issues associated with CAPPS II need to be clearly recognized and addressed before the startup of the system is authorized. These are indispensable considerations in the development of CAPPS II.

AIR TRANSPORT ASSOCIATION OF AMERICA, INC.***CAPPS2 Passenger Privacy Principles***

CAPPS2 should meet the following personal privacy safeguards before it is implemented:

1. TSA shall ensure that it only collects personal information from passengers that is (a) directly relevant to the aviation security purpose for which it is collected and (b) clearly necessary to achieve that purpose.
2. TSA shall ensure that personal information that it collects is accurate and that collected information is disposed of securely and promptly after the passenger's air transportation is completed.
3. TSA shall inform passengers: (a) why it is requiring the collection of the personal information; (b) how it will use that information; (c) the circumstances under which it will provide that information to third parties, whether those parties are private sector or governmental; and (d) its information retention and disposal policy.
4. The government shall only use collected information for aviation security purposes and shall not use the information for law enforcement purposes not directly related to aviation security.
5. TSA shall provide passengers with effective and expeditious means to (a) inquire about TSA's CAPPS2 privacy policy; (b) access, consistent with national security considerations, to their personal information and correct that information; and (c) resolve complaints about the collection, accuracy, processing, or use of personal information.
6. TSA shall take necessary steps to keep personal information secure. Such procedures shall be designed to prevent the unauthorized access to, or loss, misuse, unauthorized disclosure or alteration of, such information.
7. TSA shall not implement CAPPS 2 for international flights until it obtains any necessary determinations from foreign data protection authorities that the collection, transmission and use of information that is collected in that country for CAPPS 2 is permissible.



AIR TRANSPORT ASSOCIATION

■ JAMES C. MAY
PRESIDENT AND CEO

April 5, 2004

Hon. John L. Mica
Chairman, Aviation Subcommittee
Committee on Transportation & Infrastructure
U.S. House of Representatives
Washington, DC 20515

Re: Response to Question from March 17 Hearing on CAPPS II

Dear Chairman Mica:

At the March 17 hearing concerning the status of the Computer Assisted Passenger Prescreening System (CAPPS II) program, you asked the following question (paraphrasing): If TSA promulgates a rule requiring airlines to turn over passenger information, is that rule alone sufficient to protect the airlines from liability for disclosing confidential passenger information, or will ATA's members look for additional protection? My answer is as follows:

In the Aviation and Transportation Security Act (ATSA), Congress gave the TSA Administrator (formerly the Department of Transportation Under Secretary of Transportation for Security) broad authority to ensure the security of commercial air transportation. Thus, Congress directed the Administrator to:

- "provide for the screening of all passengers and property" carried aboard aircraft, (49 U.S.C. § 44901(a));
- "prescribe regulations to protect passengers and property on an aircraft...against an act of criminal violence or aircraft piracy" (49 U.S.C. 44903(b));
- "assess [with the Director of the FBI] current and potential threats to the domestic air transportation system. The assessment shall include consideration of the extent to which there are individuals with the capability and intent to carry out terrorist or related unlawful acts against that system..." (49 U.S.C. 44904(a));
- "assess threats to transportation," (49 U.S.C. § 114(f)(2)); and

■
AIR TRANSPORT ASSOCIATION OF AMERICA, INC.

1301 PENNSYLVANIA AVENUE, NW SUITE 1100 WASHINGTON, DC 20004-1707
202.626.4168 FAX 202.626.4166

Hon. John L. Mica
 April 5, 2004
 Page 2

- “carry out such other duties, and exercise such other powers, relating to transportation security as the [Administrator] considers appropriate, to the extent authorized by law (49 U.S.C. § 114(f)(15)).

More specifically, in ATSA Congress addressed computer assisted passenger prescreening systems and the related topic of obtaining passenger information for security purposes. Congress directed the Administrator to consider, in consultation with the Transportation Security Oversight Board, “requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security.” 49 U.S.C. 114(h)(4). Furthermore, Congress directed the Administrator to “ensure” that CAPPS I “or any successor system ... is used to evaluate all passengers before they board an aircraft,” and that individuals selected as a result of that evaluation are adequately screened. 49 U.S.C. 44903(j).

In light of TSA’s broad responsibility for security, its broad grant of authority to fulfill that responsibility, and the specific instructions to both use a computer assisted passenger prescreening system and to consider requiring air carriers to share passenger information with Federal agencies, we believe that TSA has the authority to promulgate a rule requiring airlines to share passenger information for use in the CAPPS II program. Accordingly, we see no reason at this time why complying with a lawfully promulgated regulation would expose airlines to liability under U.S. law.

Having said that, however, it would be unrealistic to suggest that airlines will not be sued for providing required passenger information to TSA pursuant to such a rule. Indeed, in a recent trade journal article, David Sobel, general counsel for the Electronic Privacy Information Center (EPIC) and a witness at the CAPPS II hearing, stated that litigation is likely. See *Aviation Week*, March 24, 2004. While I believe airlines can and will successfully defend such lawsuits, it would be best if our members were not sued at all. For this reason, I recommend a new statutory provision that *expressly* absolves airlines of any liability for turning over passenger information pursuant to a lawfully promulgated regulation and providing for compensation of legal expenses resulting from litigation challenging carrier compliance with appropriate government mandates. Such a straightforward provision would go far in preventing lawsuits that unnecessarily consume the time and resources of both the airlines and TSA. We would welcome the opportunity to work with your staff to develop such a bill.

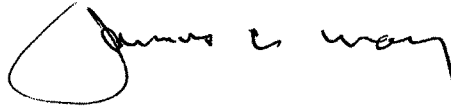
Finally, U.S. law will not protect airlines from enforcement action, and possibly criminal or civil liability, for violations of privacy obligations imposed by other countries. To the extent a TSA rule requires airlines to turn over information regarding non-US passengers traveling on international itineraries, U.S. airlines are at risk. It is imperative that the United States finalize agreements with its aviation partners to protect airlines from any administrative, criminal or civil liability risk from a foreign government. The European

Hon. John L. Mica
April 5, 2004
Page 3

Parliament's non-binding rejection last week of a US-EU accord on passenger data underscores the enforcement risk that airlines face. I recognize that these are difficult issues, but they must be resolved to protect airlines who comply with TSA or other Federal agency regulations.

Thank you for this opportunity to supplement my written statement.

Sincerely,

A handwritten signature in black ink, appearing to read "John L. Mica". The signature is written in a cursive style with a large, looping initial "J".

Testimony of
Kevin P. Mitchell
Chairman, Business Travel Coalition
Regarding CAPPS II
Before the U.S. House of Representatives
Committee on Transportation and Infrastructure
Subcommittee on Aviation
March 17, 2004

Mr. Chairman and Members of the Committee, thank you for scheduling this hearing regarding the Computer Assisted Passenger Prescreening System (CAPPS II). My name is Kevin Mitchell. I am chairman of the Business Travel Coalition (BTC), which represents the interests of major corporate buyers of commercial air transportation services.

Today, BTC testimony additionally represents the concerns of more than 100 individual travel industry supplier, distributor and technology firms who were Signatories to a letter recently transmitted to this Subcommittee regarding CAPPS II.

BTC testimony also represents the interests of travel industry associations representing thousands of European Union corporations and travel agencies with aggregate business travel purchases of some \$20 billion dollars. These associations service U.S.-based and foreign-based corporations that have employees who are citizens of other countries and who travel to and within the U.S., and sometimes work here for extended periods of time.

The following associations join with BTC in its Statement this morning:

The Institute of Travel Management that represents 1,000 business travel managers, buyers and suppliers in the UK and Ireland;

The Business Travel Association of Germany that represents more than 400 member companies; and

The Guild of Business Travel Agents which accounts for 75% of UK travel management company purchases and represents members such as American Express, Carlson Wagonlit and BTI-UK.

The business traveler, and those organizations that fund business travel activities, would ultimately be burdened with the majority of direct costs of CAPPS II in the forms of taxes, fees and ticket prices. Should the system be plagued with inaccuracies, the cost of disruptions to the conduct of business would also be born by these airlines' best customers. Firms in the travel industry distribution business face unknowable costs at this time to reconfigure their systems in accordance with the requirements of a CAPPS II.

There may be compelling rationale for revamping the current passenger prescreening system that BTC and other interested parties could support. However, as the GAO report and other analyses point out, we do not yet know in a comprehensive way what CAPPS II would be. That is to say we do not understand the privacy and civil liberty tradeoffs required in return for expectations of greater security.

Nor do we know about the safeguards, remedies, costs, future program growth and alternatives associated with such an unparalleled program.

Current concerns of aviation system customers and other stakeholders regarding CAPPS II fall into three main categories: 1) transparency and public policy debate regarding program design, 2) potential system cost and effectiveness, and 3) due process and privacy protections. This morning we will offer our assessment of these concerns as well as recommendations that would address them.

TRANSPARENCY AND DEBATE

Some 88% of participants in a recent BTC survey indicated that CAPPS II has been insufficiently debated on a national or international basis. CAPPS II has received relatively little press attention and most U.S. citizens as well as other countries' citizens who travel to and within the U.S. are simply unknowledgeable about the program, its costs and its short and long-term implications. This hearing will serve to elevate awareness and encourage further debate.

By transparency, we do not mean that we want would-be terrorists to understand details such that a system could be outsmarted. Rather, we seek transparency sufficient to know that respected experts in privacy, security, technology, cost accounting and travel industry distribution are centrally involved in developing the best CAPPS II design possible. Furthermore, we seek assurances that Congress would maintain joint accountability with TSA for ongoing program review.

CAPPS II could reach a historic threshold of intrusion on privacy rights that argues for extraordinary oversight. Throughout history, in times of national crisis, the U.S. government often emplaced policies and programs that had the effect of infringing on personal privacy and liberty. Sometimes, as in the case of Japanese Americans during World War II, the cost was dear. Historically, as crises abated, though, policies that infringed upon freedoms were likewise rolled back, or eliminated.

Unlike temporary programs to frustrate past U.S. enemies, CAPPS II, as a response in the U.S. War on Terrorism, is being viewed as permanent in nature; as if the War will be permanent. By definition, if CAPPS II is to be effective, it must be powerful, adaptable and somewhat secretive. By its nature, a government agency that manages a program such as CAPPS II would over time likely seek to expand the program's capabilities and applications while endeavoring to avoid public scrutiny.

For example, if major U.S. infrastructure facilities were successfully attacked via a gasoline tanker, it would be claimed quickly that a version of CAPPS II should be implemented at interstate toll booths. Likewise, if suicide bombers began targeting Amtrak trains, passengers could expect to be color-coded at train stations. Sporting events, political rallies and other venues where freedoms are celebrated could soon follow.

In the final analysis, these steps might indeed be rational and effective ones to take in a continuing War on Terrorism. However, the mere possibility of these unfortunate developments underscores the need for a thorough public policy debate prior to CAPPS II implementation so that all Americans and foreign citizens understand the program and accept the many potentially serious implications.

Importantly, given the program's current scope, permanency and opportunity for expansion, consideration needs to be given to the circumstances under which Congress might be able to determine that the War on Terrorism has been won so that CAPPS II could be rolled back. After all, President Bush states that the War will be won. Alternatively, if less invasive alternatives to CAPPS II become available, a formal mechanism is needed to override natural bureaucratic tendencies to resist change and protect power.

SYSTEM COST AND EFFECTIVENESS

A program with such potentially far reaching consequences such as CAPPS II requires an understanding of the projected total direct and indirect costs over a multi-year time horizon. Knowing the

required resources of money, expertise, time and computing capacity would assist in evaluating alternative uses of these resources in other problematic areas of aviation security, such as cargo.

On a more basic level, and beyond the proposed TSA CAPPS II testing phase, we need to know if the program would actually make aviation system security sufficiently better when considering the resources required and the tradeoffs in personal privacy and freedoms.

BTC research since 2001 has demonstrated that business travelers are willing to give up some privacy for security if it can be proven that they would really be more secure. This important burden of proof should be on the government.

Respected international aviation security experts raise the following concerns regarding the potential effectiveness of CAPPS II:

- **Over Reliance on Technology.** In the view of former El Al airline global security chief Issac Yeffet, the U.S. is currently over reliant on technology, and not very good technology, at airports for carry-on and checked baggage screening, at the expense of developing human expertise. At issue is once CAPPS II is implemented, how would passengers who are color-coded yellow be further processed? As Yeffet states, "Who will interview you? Who will do the investigation? Who will determine who is suspicious when we only train people how to operate x-ray machines and do body searches only when the alarm goes off?"
- **Value of ID Checks.** Ostensibly, identification systems seek to identify and create two categories of people—potential good guys and potential bad guys. With CAPPS II, the first category (green) contains passengers requiring little screening and the second category (yellow and red) includes passengers that require additional screening measures. However, this kind of system creates a third and dangerous category: Bad guys that do not fit the profile.

As chief technology officer at Counterpane Internet Security, and identification expert Bruce Schneier states, "Oklahoma City bomber Timothy McVeigh, Washington-area sniper John Allen Muhammed and many of the Sept. 11 terrorists had no previous links to terrorism. The Unabomber taught mathematics at UC Berkeley. Profiling can result in less security by giving certain people an easy way to skirt security."

Of concern is that a U.S.-based Al-Qaeda sleeper cell could throw 50 recruits at a CAPPS II until it identified 10 that were color-coded green. Once a person is color-coded green, it follows that he or she would always be categorized as such until and unless something fundamental changes in the person's profile. Such a system could not only provide a false sense of security at considerable economic and non-economic costs, but it could actually reduce our absolute level of security.

- **Reduction of Randomness.** TSA states that as a benefit of CAPPS II the current 15% of passengers who are flagged for secondary screening would be reduced to just 2% to 3%. Security experts worldwide consider the possibility of random selection for secondary screening to be a best-practice deterrent vis-à-vis would-be terrorists. Benefits from CAPPS II could be outweighed by the loss of this deterrent.

DUE PROCESS AND PRIVACY PROTECTIONS

There are numerous serious privacy and civil liberty concerns that privacy groups and others have raised that BTC shares. I would like to focus, however, on just those concerns expressed by the Signatories to the letter BTC recently sent to this Committee as well as the concerns of industry associations previously listed.

- **Secrecy.** TSA is seeking exemptions from the Privacy Act for the CAPPS II program without providing sufficient rationale. So, from the outset, privacy protections would appear to be diluted. Moreover, CAPPS II places the riskiest aspect of the program, the determination of risk and the construction of rules for conducting background checks, into the purview of

secretive intelligence and law enforcement programs and databases. This operating platform reinforces suspicion and concern that CAPPS II would be beyond reasonable public review and oversight.

- **Profile Mistakes.** How would a passenger challenge his risk assessment score and how long would it take to correct inaccuracies in one's profile? It is extremely worrisome to business travelers from around the world that erroneous information in databases might result in their being perpetually flagged for extra screening. With TSA's recently announced policy that a passenger with a bad attitude could have hefty fines levied against him, it would seem that some passengers would be set on a collision course with the U.S. government.

This issue is particularly important to U.S. and foreign-based corporations that have employees who are citizens of other countries who travel to and within the U.S. and sometimes work here for extended periods of time. What extra steps would a foreigner be required to take, and at what expense, to prove that he is low risk to the U.S. aviation system? If one member of a group traveling together is color-coded yellow or red, would the entire group receive additional screening?

Importantly, Islam is the fastest growing religion among African Americans, many of whom are business travelers. Often conversion to Islam leads to a name change of the kind that could be mistaken for names on various terrorist watch lists. What assurance would there be that such individuals would have access to timely and complete corrections to their records?

TSA is currently in a disagreement with the airlines over who should pay for lost, stolen or damaged luggage. Passengers have claims that are 18 months old, and still unresolved. So, if TSA cannot do right by passengers with a simple compensation issue over luggage, how are passengers to have confidence that they would have better results with correcting inaccuracies in their risk profiles?

- **The Cost of Mistakes.** Who would pay for false-positive related travel disruptions when a business traveler who consistently scores yellow for unknown and unresolved reasons consequently misses scheduled flights? Who would be responsible for the additive cost of thousands of dollars for walk-up fares required for subsequently scheduled flights? Would a traveler's employer patiently wait 18 months or longer for the traveler to rectify his record with the TSA? The overall cost to a corporation from lost business opportunities could be considerable.

RECOMMENDATIONS

1. CAPPS II should be strictly authorized for use only in aviation system security.
2. The process and timeframe for U.S. citizens and foreigners to have their risk profiles corrected needs to be efficient-to-a-fault, and ironclad.
3. The threshold requirements that Congress wisely placed on the TSA for CAPPS II to be fully funded should be revised to reflect GAO's recently published CAPPS II audit results as well as the ideas and concerns that will come to light from a thorough public policy debate.
4. An organization such as GAO, answerable only to Congress, should have sufficient national security clearances and attendant authority to monitor all aspects of a CAPPS II including policies, programs and practices of other supporting government agencies and private sector contractors.
5. CAPPS II should be sunsetted after 3 to 5 years to enable Congress to carefully evaluate the costs, efficacy and ongoing need for the program and determine if it warrants reauthorization.

Thank you for the opportunity to provide this testimony.

**THE HONORABLE JAMES L. OBERSTAR
RANKING DEMOCRATIC MEMBER
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE**

**STATEMENT ON THE
COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM (CAPPS II)
MARCH 17, 2004**

Thank you, Chairman Mica and Ranking Member DeFazio, for convening this hearing today on aviation security. Today, we are focused on the Computer Assisted Passenger Pre-Screening System, or CAPPS II, which is a tool that will be used by the Transportation Security Administration (TSA) to select passengers and their baggage for extra security screening.

Since 1998, the airlines have used the CAPPS system to identify passenger baggage for extra security measures – an effort spearheaded by Northwest Airlines in 1994, with grants made available by the Federal Aviation Administration (FAA). Interest in a computer selection system was spurred initially by concerns that a terrorist act was responsible for the TWA 800 explosion. In 1996, then-President Clinton organized the White House Commission on Aviation Safety and Security (the Gore Commission), including using computer selection of passengers to complement screening by explosive detection systems. Congress acted on many of the Gore

Commission recommendations and, in the 1996 FAA Reauthorization Act, directed the FAA to assist the airlines in what became the CAPPs system.

Now, we are focusing on CAPPs II, the next generation CAPPs system. The CAPPs II system will draw on both commercial and government databases to authenticate a passenger's identity and determine whether that person poses a risk to aviation and should receive extra scrutiny. The CAPPs II system will request an identity authentication from commercial data providers, focusing on a passenger's name, address, birth date, and telephone number. CAPPs II will then conduct a risk assessment using government databases, including classified and intelligence data, to generate a risk score. Based on that score, a person will be categorized as an acceptable risk, unknown risk, or unacceptable risk. Passengers posing an unknown risk will receive extra scrutiny, while passengers posing an unacceptable risk will be denied boarding.

At the outset, I am skeptical that the CAPPs II system will be able to account for the long-term terrorists or "sleeper" cells that we all know exist in the United States. It is not too hard to imagine that a terrorist could live under an assumed identity for years with a fake name, address, telephone number and date of birth that could evade suspicion in the CAPPs II database. The General Accounting Office (GAO), in its recent report on the CAPPs II system, cited identity theft as an area of

concern. I look forward to hearing more from the GAO as well as the TSA on this issue.

I have long urged the FAA, and now the TSA, to follow the fourteen-year-old recommendations of the Pan Am Commission that the United States become more aggressive in our intelligence gathering, evaluation, and dissemination and target the information used to specific rather than general threats. Quoting from the report,

The Commission also recommends greater emphasis within the intelligence community on developing a specific union whose principle function will be long-term strategic thinking and planning on terrorism. The objective is to be better able to anticipate future terrorist strategies and tactics, rather than simply to react to incidents as they occur.

The skills of terrorists have stepped up several levels since the Commission's 1990 report. We must ensure that our counter-intelligence rises to meet that threat, and that intelligence gathered is properly disseminated to the transportation modes. Without the intelligence, the TSA will not be able to meet the technology and other challenges associated with security threats. To that end, ATSA requires the coordination, sharing and dissemination of intelligence information among federal agencies. I again urge that meaningful steps be taken to integrate the sharing of threat

data between the intelligence and transportation communities, and would hope that the CAPPs II system will be able to take advantage of enhanced intelligence gathering.

Many other serious issues have been raised about the CAPPs II system, including privacy concerns; redress procedures to assist passengers when they have mistakenly been identified as a false positive in the system; general data accuracy; and mission creep. I look forward to having these issues addressed by the TSA.

Whether CAPPs II will prove to be a useful tool in the fight against terrorism remains to be seen. I believe that we must continue to bolster TSA's efforts to develop next generation screening technologies. ATSA increased authorized funding to accelerate the development of new screening technologies, and we should continue to provide stringent oversight to ensure that such technologies are deployed at our nation's airports.

I thank the Chairman and the Ranking Member for holding this timely hearing and I look forward to hearing the witnesses' testimony.

Statement of
Honorable Stevan Pearce
Of New Mexico
in Subcommittee on Aviation
House Transportation and Infrastructure Committee
Hearing on Computer Assisted Passenger Prescreening Service (CAPPS II)

Mr. Chairman, thank you for holding the hearing today on the status of the Computer Assisted Passenger Prescreening System (CAPPS II). The terrorist events in Madrid last week further illuminate our responsibility to ensure effective passenger screening capabilities in a timely manner.

We are all here today to evaluate the progress made to date on addressing concerns regarding privacy, due process, accuracy and efficacy of the CAPPS II system.

I originally assumed while looking over all of the pre-hearing materials that very little *progress* on implementing an effective system had been made due to the sustained, misdirected and suppressive nature of conflicts over privacy and due process.

While these are all critical questions that must be asked and problems that must be resolved, my inclination is that accuracy and efficacy, can be resolved relatively easily and timely. It is the privacy issues that are preventing the accuracy and efficacy from ever moving forward and the due process demands that will prevent the project from ever getting off the ground.

My original assumptions about the outcome of this hearing are being reconfirmed by most of my colleagues' opening statements here today.

On one side of their mouths, my colleagues berate the Transportation Security Administration for their inefficiency and reiterate the urgency of effective prescreening capabilities to prevent another tragic attack on lives through aviation like what occurred on September 11th. On the other side of their mouths, my colleagues prefer CAPPS II be hostage to trial attorneys and litigation.

The terrorists used America's aviation security screening system against us with devastating consequences—\$2 trillion cost to our economy, and 3,000 lives lost.

The terrorists' impact on September 11th will pale in comparison to how they will again use our aviation security system to attack us if it is handicapped by trial lawyers and excessive litigation to the point of ineffectiveness.

Now, I am not advocating less responsibility and vigilance on behalf of the Transportation Security Administration to address the privacy issues with CAPPS II. While there are legitimate reasons for requesting Privacy Act exemptions, these reasons are being trivialized and undermined by the TSA's inability to communicate effectively

and following the proper procedures for disclosure to the public for the reasons behind the exemption request.

All parties to this matter—Congress, the Administration, and the public—must be responsible in closing the opportunities for any terrorist to use our aviation security system to our detriment ever again.

STEVAN PEARCE
Member of Congress

United States General Accounting Office

GAO

Testimony
Before the Subcommittee on Aviation,
Committee on Transportation and
Infrastructure, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, March 17, 2004

AVIATION SECURITY

Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System

Statement of Norman J. Rabkin, Managing Director,
Homeland Security and Justice Issues and
David A. Powner, Director, Information Technology Issues



GAO-04-504T

GAO
Accountability Integrity Reliability
Highlights

Highlights of GAO-04-504T, a testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

The security of U.S. commercial aviation is a long-standing concern, and substantial efforts have been undertaken to strengthen it. One such effort is the development of a new Computer-Assisted Passenger Prescreening System (CAPPS II) to identify passengers requiring additional security attention. The development of CAPPS II has raised a number of issues, including whether individuals may be inappropriately targeted for additional screening and whether data accessed by the system may compromise passengers' privacy. GAO was asked to summarize the results of its previous report that looked at (1) the development status and plans for CAPPS II; (2) the status of CAPPS II in addressing key developmental, operational, and public acceptance issues; and (3) additional challenges that could impede the successful implementation of the system.

What GAO Recommends

In a recent report (GAO-04-385), GAO recommended that the Secretary of the Department of Homeland Security (DHS) develop project plans, including schedules and estimated costs; a plan for completing critical security activities; a risk mitigation strategy for system testing; policies governing program oversight; and a process by which passengers can correct erroneous information. DHS generally concurred with the report and its recommendations.

www.gao.gov/cgi-bin/gettrpt?GAO-04-504T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkin@gao.gov or David Pownier at (202) 512-9286 or pownierd@gao.gov.

March 2004

AVIATION SECURITY

Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System

What GAO Found

Key activities in the development of CAPPS II have been delayed, and the Transportation Security Administration (TSA) has not yet completed important system planning activities. TSA is currently behind schedule in testing and developing initial increments of CAPPS II, due in large part to delays in obtaining needed passenger data for testing from air carriers because of privacy concerns. TSA also has not established a complete plan identifying specific system functionality that will be delivered, the schedule for delivery, and estimated costs. The establishment of such plans is critical to maintaining project focus and achieving intended results within budget. Without such plans, TSA is at an increased risk of CAPPS II not providing the promised functionality, of its deployment being delayed, and of incurring increased costs throughout the system's development.

TSA also has not completely addressed seven of the eight issues identified by the Congress as key areas of interest related to the development, operation, and public acceptance of CAPPS II. Although TSA is in various stages of progress on addressing each of these eight issues, as of January 1, 2004, only one—the establishment of an internal oversight board to review the development of CAPPS II—has been completely addressed. However, concerns exist regarding the timeliness of the board's future reviews. Other issues, including ensuring the accuracy of data used by CAPPS II, stress testing, preventing unauthorized access to the system, and resolving privacy concerns have not been completely addressed, due in part to the early stage of the system's development. See table below for a summary of TSA's status in addressing the eight key legislative issues.

Status of TSA in Addressing Key Legislative Issues as of January 1, 2004

Fully addressed	Yes	No	Fully addressed	Yes	No
Oversight board	✓		Unauthorized access prevention		✓
Accuracy of data		✓	Policies for operation and use		✓
Stress testing		✓	Privacy concerns resolved		✓
Abuse prevention		✓	Redress process		✓

Source: GAO

GAO identified three additional challenges TSA faces that may impede the success of CAPPS II. These challenges are developing the international cooperation needed to obtain passenger data, managing the possible expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system. GAO believes that these issues, if not resolved, pose major risks to the successful deployment and implementation of CAPPS II.

Mr. Chairman and Members of the Subcommittee:

The security of our nation's commercial aviation system has been a long-standing concern. For over 30 years, numerous efforts have been undertaken to improve aviation security, but weaknesses persist. Following the tragic events of September 11, 2001, substantial changes were made to strengthen aviation security and reduce opportunities for terrorists to hijack or destroy commercial aircraft. However, as recent flight cancellations over the last 3 months have shown, the threat of terrorist attempts to use commercial aircraft to inflict casualties and damage remains. With thousands of daily flights carrying millions of passengers, ensuring that no passenger poses a threat to commercial aviation remains a daunting task.

My testimony today focuses on the development of and challenges facing one particular effort underway to strengthen aviation security—the new Computer-Assisted Passenger Prescreening System (CAPPS II). More specifically, my testimony highlights three key areas: (1) the development status and plans for CAPPS II, (2) the status of CAPPS II in addressing eight program issues of particular concern to the Congress, and (3) additional challenges that pose major risks to the development and implementation of the system. My testimony is based on our recently issued report¹ and, because the development of CAPPS II is ongoing, updated information we have acquired since our report's issuance.

In summary, we found that:

- Key activities in the development of CAPPS II have been delayed, and the Department of Homeland Security's (DHS) Transportation Security Administration (TSA)—the agency responsible for developing CAPPS II—has not yet completed important system planning activities. TSA is currently behind schedule in testing and developing the initial phases—called increments—of CAPPS II due in large part to delays in obtaining needed passenger data for testing from air carriers because of privacy concerns. Furthermore, the system's initial operating capability—the point at which the system will be ready to operate with data from one airline—has been postponed and a new date has not been determined. TSA also has not yet established a complete plan that identifies specific system

¹U.S. General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 (Washington, D.C.: Feb. 12, 2004).

functions that it will deliver, the schedule for delivery, and the estimated costs throughout the system's development. Establishing such plans is critical to maintaining project focus and achieving intended system results. Project officials reported that they have developed cost and schedule plans for initial increments, but are unable to plan for future increments with any certainty due to testing delays.

- TSA has not fully addressed seven of eight CAPPS II issues identified by the Congress as key areas of interest, due in part to the early stage of the system's development. The one issue that has been addressed involves the establishment of an internal oversight board to review the development of major systems, including CAPPS II. DHS and TSA are taking steps to address the remaining seven issues; however, they have not yet
 1. determined and verified the accuracy of the databases to be used by CAPPS II,
 2. stress tested and demonstrated the accuracy and effectiveness of all search tools to be used by CAPPS II,
 3. developed sufficient operational safeguards to reduce the opportunities for abuse,
 4. established substantial security measures to protect CAPPS II from unauthorized access by hackers and other intruders,
 5. adopted policies to establish effective oversight of the use and operation of the system,
 6. identified and addressed all privacy concerns, and
 7. developed and documented a process under which passengers impacted by CAPPS II can appeal decisions and correct erroneous information.
- In addition to facing developmental and operational challenges related to the key areas of interest of the Congress, CAPPS II also faces a number of additional challenges that may impede its success. These challenges are developing the international cooperation needed to obtain passenger data, managing the expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system.

Background

During the late 1960s and early 1970s, the government directed that all passengers and their carry-on baggage be screened for dangerous items before boarding a flight. As the volume of passengers requiring screening increased and an awareness of terrorists' threats against the United States developed, a computerized system was implemented in 1998 to help identify passengers posing the greatest risk to a flight so that they could receive additional security attention. This system, known as CAPPS,² is operated by air carriers in conjunction with their reservation systems. CAPPS enables air carriers to separate passengers into two categories: those who require additional security screening—termed “selectees”—and those who do not. Certain information contained in the passenger's reservation is used by the system to perform an analysis against established rules and a government supplied “watch list” that contains the names of known or suspected terrorists. If the person is deemed to be a “selectee,” the boarding pass is encoded to indicate that additional security measures are required at the screening checkpoint. This system is currently used by most U.S. air carriers to prescreen passengers and prescreens an estimated 99 percent of passengers on domestic flights. For those passengers not prescreened by the system, certain air carriers manually prescreen their passengers using CAPPS criteria and the watch list.

Following the events of September 11, 2001, Congress passed the Aviation and Transportation Security Act³ requiring that a computer-assisted passenger prescreening system be used to evaluate all passengers. TSA's Office of National Risk Assessment has undertaken the development of a second-generation computer-assisted passenger prescreening system, known as CAPPS II. Unlike the current system that is operated by the air carriers, the government will operate CAPPS II. Further, it will perform different analyses and access more diverse data, including data from commercial and government databases, to classify passengers according to their level of risk.

TSA program officials expect that CAPPS II will provide significant improvements over the existing system. First, they believe a centralized CAPPS II that will be owned and operated by the federal government will allow for more effective and efficient use of up-to-date intelligence

²When initially developed by the Federal Aviation Administration, this system was known as the Computer-Assisted Passenger Screening system or CAPS.

³Pub. L. No. 107-71, § 136, 115 Stat. 597, 637 (2001).

information and make CAPPS II more capable of being modified in response to changing threats. Second, they also believe that CAPPS II will improve identity authentication and reduce the number of passengers who are falsely identified as needing additional security screening. Third, CAPPS II is expected to prescreen all passengers on flights either originating in or destined for the United States. Last, an additional expected benefit of the system is its ability to aggregate risk scores to identify higher-risk flights, airports, or geographic regions that may warrant additional aviation security measures.

**System Development
Behind Schedule and
Critical Plans
Incomplete**

Key activities in the development of CAPPS II have been delayed, and TSA has not yet completed key system planning activities. TSA plans to develop CAPPS II in nine increments, with each increment providing increased functionality. (See app. I for a description of these increments.) As each increment is completed, TSA plans to conduct tests that would ensure the system meets the objectives of that increment before proceeding to the next increment. The development of CAPPS II began in March 2003 with increments 1 and 2 being completed in August and October 2003, respectively. However, TSA has not completely tested these initial two increments because it was unable to obtain the necessary passenger data for testing from air carriers. Air carriers have been reluctant to provide passenger data due to privacy concerns. Instead, the agency deferred completing these tests until increment 3.

TSA is currently developing increment 3. However, due to the unavailability of passenger data needed for testing, TSA has delayed the completion of this increment from October 2003 until at least the latter part of this month and reduced the functionality that this increment is expected to achieve. Increment 3 was originally intended to provide a functioning system that could handle live passenger data from one air carrier in a test environment to demonstrate that the system can satisfy operational and functional requirements. However, TSA officials reported that they recently modified increment 3 to instead provide a functional application of the system in a simulated test environment that is not actively connected to an airline reservation system. Officials also said that they were uncertain when the testing that was deferred from increments 1 and 2 to increment 3 will be completed. TSA recognizes that system testing is a high-risk area and plans to further delay the implementation of the system to ensure that sufficient testing is completed. As a result, all succeeding increments of CAPPS II have been delayed, moving CAPPS II initial operating capability—the point at which the system will be ready to operate with one airline—from November 2003 to a date unknown. (See

app. II for a timeline showing the original and revised schedule for CAPPS II increments.)

Further, we found that TSA has not yet developed critical elements associated with sound project planning, including a plan for what specific functionality will be delivered, by when, and at what cost throughout the development of the system. Our work on similar systems and other best practice research have shown that the application of rigorous practices to the acquisition and development of information systems improves the likelihood of the systems' success. In other words, the quality of information technology systems and services is governed largely by the quality of the processes involved in developing and acquiring the system. We have reported that the lack of such practices has contributed to cost, schedule, and performance problems for major system acquisition efforts.⁴

TSA established plans for the initial increments of the system, including requirements for increments 1 and 2 and costs and schedules for increments 1 through 4. However, officials lack a comprehensive plan identifying the specific functions that will be delivered during the remaining increments; for example, which government and commercial databases will be incorporated, the date when these functions will be delivered, and an estimated cost of the functions. In addition, TSA officials recently reported that the expected functionality to be achieved during early increments has been reduced, and officials are uncertain when CAPPS II will achieve initial operating capability. Project officials also said that because of testing delays, they are unable to plan for future increments with any certainty.

By not completing these key system development planning activities, TSA runs the risk that CAPPS II will not provide the full functionality promised. Further, without a clear link between deliverables, cost, and schedule, it will be difficult to know what will be delivered and when in order to track development progress. Until project officials develop a plan that includes scheduled milestones and cost estimates for key deliverables, CAPPS II is at increased risk of not providing the promised functionality, not being fielded when planned, and being fielded at an increased cost.

⁴U.S. General Accounting Office, *Major Management Challenges and Program Risks: A Government-wide Perspective*, GAO-03-95 (Washington, D.C.: January 2003) and *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

Developmental, Operational, and Privacy Issues Identified by the Congress Remain Unresolved

In reviewing CAPPS II, we found that TSA has not fully addressed seven of the eight issues identified by the Congress as key areas of interest related to the development and implementation of CAPPS II. Public Law 108-90 identified eight key issues⁵ that TSA must fully address before the system is deployed or implemented. These eight issues are

- establishing an internal oversight board,
- assessing the accuracy of databases,
- testing the system load capacity (stress testing) and demonstrating its efficacy and accuracy,
- installing operational safeguards to protect the system from abuse,
- installing security measures to protect the system from unauthorized access,
- establishing effective oversight of the system's use and operations,
- addressing all privacy concerns, and
- creating a redress process for passengers to correct erroneous information.

While TSA is in various stages of progress to address each of these issues, only the establishment of an internal oversight board to review the development of CAPPS II has been fully addressed. For the remaining issues, TSA program officials contend that their ongoing efforts will ultimately address each issue. However, due to system development delays, uncertainties regarding when passenger data will be obtained to test the system, and the need to finalize key policy decisions, officials were unable to identify a time frame for when all remaining issues will be fully addressed.

The following briefly summarizes the status of TSA's efforts to address each of the eight issues.

⁵Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003).

-
- Establishment of a CAPPS II oversight board has occurred.

DHS created an oversight board—the Investment Review Board—to review the department's largest capital asset programs. The Board reviewed CAPPS II in October 2003. Based on this review, the Board authorized TSA to proceed with the system's development. However, DHA noted some areas that the program needed to address. These areas included addressing privacy and policy issues, coordinating with other stakeholders, and identifying program staffing requirements and costs, among others, and directed that these issues be addressed before the system proceeds to the next increment.

Although DHS has the Board in place to provide internal oversight and monitoring for CAPPS II and other large capital investments, we recently reported that concerns exist regarding the timeliness of its future reviews. DHS officials acknowledged that the Board is having difficulty reviewing all of the critical departmental programs in a timely manner.⁶ As of January 2004, DHS had identified about 50 of the largest capital assets that would be subject to the Board's review. As CAPPS II's development proceeds, it will be important for the Board to oversee the program on a regular and thorough basis to provide needed oversight.

In addition, on February 12, 2004, DHS announced its intentions to establish an external review board specifically for CAPPS II. This review board will be responsible for ensuring that (1) the privacy notice is being followed, (2) the appeal process is working effectively, and (3) the passenger information used by CAPPS II is adequately protected. However, in announcing the establishment of this review board, DHS did not set a date as to when the board will be activated or who would serve on the board.

- The accuracy of CAPPS II databases has not yet been determined.

TSA has not yet determined the accuracy—or conversely, the error rate—of commercial and government databases that will be used by CAPPS II. Since consistent and compatible information on database accuracy is not available, TSA officials said that they will be developing and conducting their own tests to assess the overall accuracy of information contained in

⁶U.S. General Accounting Office, *Information Technology: OMB and Department of Homeland Security Investment Reviews* GAO-04-323 (Washington, D.C.: Feb. 10, 2004).

commercial and government databases. These tests are not intended to identify all errors existing within a database, but rather assess the overall accuracy of a database before determining whether it is acceptable to be used by CAPPS II.

In addition to testing the accuracy of commercial databases, TSA plans to better ensure the accuracy of information derived from commercial databases by using multiple databases in a layered approach to authenticating a passenger's identity. If available information is insufficient to validate the passenger's identification in the first database accessed, then CAPPS II will access another commercial database to provide a second layer of data, and if necessary, still other commercial databases. However, how to better ensure the accuracy of government databases will be more challenging. TSA does not know exactly what type of information the government databases contain, such as whether a database will contain a person's name and full address, a partial address, or no address at all. A senior program official said that using data without assessing accuracy and mitigating data errors could result in erroneous passenger assessments; consequently government database accuracy and mitigation measures will have to be developed and completed before the system is placed in operation.

In mitigating errors in commercial and government databases, TSA plans to use multiple databases and a process to identify misspellings to correct errors in commercial databases. TSA is also developing a redress process whereby passengers can attempt to get erroneous data corrected. However, it is unclear what access passengers will have to information found in either government or commercial databases, or who is ultimately responsible for making corrections. Additionally, if errors are identified during the redress process, TSA does not have the authority to correct erroneous data in commercial or government databases. TSA officials said they plan to address this issue by establishing protocols with commercial data providers and other federal agencies to assist in the process of getting erroneous data corrected.

- Stress testing and demonstration of the system's efficacy and accuracy have been delayed.

TSA has not yet stress tested CAPPS II increments developed to date or conducted other system-related testing to fully demonstrate the effectiveness and accuracy of the system's search capabilities, or search tools, to correctly assess passenger risk levels. TSA initially planned to conduct stress testing on an early increment of the system by August 2003.

However, stress testing was delayed several times due to TSA's inability to obtain the 1.5 million Passenger Name Records it estimates are needed to test the system. TSA attempted to obtain the data needed for testing from three different sources but encountered problems due to privacy concerns associated with its access to the data. For example, one air carrier initially agreed to provide passenger data for testing purposes, but adverse publicity resulted in its withdrawal from participation.

Further, as the system is more fully developed, TSA will need to conduct stress testing. For example, there is a stringent performance requirement for the system to process 3.5 million risk assessment transactions per day with a peak load of 300 transactions per second that cannot be fully tested until the system is further along in development. Program officials acknowledge that achieving this performance requirement is a high-risk area and have initiated discussions to define how this requirement will be achieved. However, TSA has not yet developed a complete mitigation strategy to address this risk. Without a strategy for mitigating the risk of not meeting peak load requirements, the likelihood that the system may not be able to meet performance requirements increases.

Other system-related testing to fully demonstrate the effectiveness and accuracy of the system's search tools in assessing passenger risk levels also has not been conducted. This testing was also planned for completion by August 2003, but similar to the delays in stress testing, TSA's lack of access to passenger data prevented the agency from conducting these tests. In fact, TSA has only used 32 simulated passenger records—created by TSA from the itineraries of its employees and contractor staff who volunteered to provide the data—to conduct this testing. TSA officials said that the limited testing—conducted during increment 2—has demonstrated the effectiveness of the system's various search tools. However, tests using these limited records do not replicate the wide variety of situations they expect to encounter with actual passenger data when full-scale testing is actually undertaken. As a result, the full effectiveness and accuracy of the tools have not been demonstrated.

TSA's attempts to obtain test data are still ongoing, and privacy issues remain a stumbling block. TSA officials believe they will continue to have difficulty in obtaining data for both stress and other testing until TSA issues a Notice of Proposed Rulemaking to require airlines to provide passenger data to TSA. This action is currently under consideration within TSA and DHS. In addition, TSA officials said that before the system is implemented, a final Privacy Act notice will be published. According to DHS's Chief Privacy Officer, the agency anticipated that the Privacy Act

notice would be finalized in March 2004. However, this official told us that the agency will not publish the final Privacy Act notice until all 15,000 comments received in response to the August 2003 Privacy Act notice are reviewed and testing results are available. DHS could not provide us a date as to when this will be accomplished. Further, due to the lack of test data, TSA delayed the stress and system testing planned for increments 1 and 2 to increment 3, scheduled to be completed by March 31, 2004. However, since we issued our report last month, a TSA official said that they no longer expect to conduct this testing during increment 3 and do not have an estimated date for when these tests will be conducted. Uncertainties surrounding when stress and system testing will be conducted could impact TSA's ability to allow sufficient time for testing, resolving defects, and retesting before CAPPS II can achieve initial operating capability and may further delay system deployment.

- Security plans that include operational and security safeguards are not complete.⁷

Due to schedule delays and the early stage of CAPPS II development, TSA has not implemented critical elements of an information system security program to reduce opportunities for abuse and protect against unauthorized access by hackers. These elements—a security policy, a system security plan, a security risk assessment, and the certification and accreditation of the security of the system—together provide a strong security framework for protecting information technology data and assets. While TSA has begun to implement critical elements of an information security management program for CAPPS II, these elements have not been completed. Until a specific security policy for CAPPS II is completed, TSA officials reported that they are using relevant portions of the agency's information security policy and other government security directives as the basis for its security policy. As for the system security plan, it is currently in draft. TSA expects to complete this plan by the time initial operating capability is achieved. Regarding the security risk assessment, TSA has postponed conducting this assessment because of development delays and it has not been rescheduled. The completion date remains uncertain because TSA does not have a date for achieving initial operating capability as a result of other CAPPS II development delays. As for final

⁷Because operational safeguards to reduce opportunities for abuse and security measures to protect CAPPS II from unauthorized access by hackers are so closely related, these two issues are discussed jointly.

certification and accreditation, TSA is unable to schedule the final certification and accreditation of CAPPs II because of the uncertainty regarding the system's development schedule.

The establishment of a security policy and the completion of the system security plan, security risk assessment, and certification and accreditation process are critical to ensuring the security of CAPPs II. Until these efforts are completed, there is decreased assurance that TSA will be able to adequately protect CAPPs II information and an increased risk of operational abuse and access by unauthorized users.

- Policies for effective oversight of the use and operation of CAPPs II are not developed.

TSA has not yet fully established controls to oversee the effective use and operation of CAPPs II. However, TSA plans to provide oversight of CAPPs II through two methods: (1) establishing goals and measures to assess the program's strengths, weaknesses, and performance and (2) establishing mechanisms to monitor and evaluate the use and operation of the system.

TSA has established preliminary goals and measures to assess the CAPPs II program's performance in meeting its objectives as required by the Government Performance and Results Act.⁶ Specifically, the agency has established five strategic objectives with preliminary performance goals and measures for CAPPs II. While this is a good first step, these measures may not be sufficient to provide the objective data needed to conduct appropriate oversight. TSA officials said that they are working with five universities to assess system effectiveness and management and will develop metrics to be used to measure the effectiveness of CAPPs II. With this information, officials expect to review and, as necessary, revise their goals and objectives to provide management and the Congress with objective information to provide system oversight.

In addition, TSA has not fully established or documented additional oversight controls to ensure that operations are effectively monitored and evaluated. Although TSA has built capabilities into CAPPs II to monitor and evaluate the system's operation and plans to conduct audits of the system to determine whether it is functioning as intended, TSA has not written all of the rules that will govern how the system will operate.

⁶Pub. L. No. 103-62, 107 Stat. 285 (1993).

Consequently, officials do not yet know how these capabilities will function, how they will be applied to monitor the system to provide oversight, and what positions and offices will be responsible for maintaining the oversight. Until these policies and procedures for CAPPS II are developed, there is no assurance that proper controls are in place to monitor and oversee the system.

- TSA's plans address privacy protection, but issues remain unresolved.

TSA's plans for CAPPS II reflect an effort to protect individual privacy rights, but certain issues remain unresolved. Specifically, TSA plans address many of the requirements of the Privacy Act, the primary legislation that regulates the government's use of personal information.⁹ For example, in January 2003, TSA issued a notice in the Federal Register that generally describes the Privacy Act system of records¹⁰ that will reside in CAPPS II and asked the public to comment. While TSA has taken these initial steps, it has not yet finalized its plans for complying with the act. For example, the act and related Office of Management and Budget guidance¹¹ state that an agency proposing to exempt a system of records from a Privacy Act provision must explain the reasons for the exemption in a published rule. In January 2003, TSA published a proposed rule to exempt the system from seven Privacy Act provisions but has not yet provided the reasons for these exemptions, stating that this information will be provided in a final rule to be published before the system becomes operational. As a result, TSA's justification for these exemptions remains unclear. Until TSA finalizes its privacy plans for CAPPS II and addresses such concerns, the public lacks assurance that the system will fully comply with the Privacy Act.

⁹Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a).

¹⁰Under the act, a system of records is a collection of information about individuals under the control of an agency from which information is actually retrieved by an individual's name or by some identifying number, symbol, or other particular assigned to the individual.

¹¹Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,972 (July 9, 1975).

When viewed in the larger context of Fair Information Practices¹²—internationally recognized privacy principles that also underlie the Privacy Act—TSA plans reflect some actions to address each of these practices. For example, TSA's plan to not collect passengers' social security numbers from commercial data providers and to destroy most passenger information shortly after they have completed their travel itinerary appears consistent with the collection limitation practice, which states that collections of personal information should be limited. However, to meet its evolving mission goals, TSA plans also appear to limit the application of certain of these practices. For example, TSA plans to exempt CAPPS II from the Privacy Act's requirements to maintain only that information about an individual that is relevant and necessary to accomplish a proper agency purpose. These plans reflect the subordination of the use limitation practice and data quality practice (personal information should be relevant to the purpose for which it is collected) to other goals and raises concerns that TSA may collect and maintain more information than is needed for the purpose of CAPPS II, and perhaps use this information for new purposes in the future. Such actions to limit the application of the Fair Information Practices do not violate federal requirements. Rather, they reflect TSA's efforts to balance privacy with other public policy interests such as national security, law enforcement, and administrative efficiency. As the program evolves, it will ultimately be up to policymakers to determine if TSA has struck an appropriate balance among these competing interests.

- Redress process is being developed, but significant challenges remain.

TSA intends to establish a process by which passengers who are subject to additional screening or denied boarding will be provided the opportunity to seek redress by filing a complaint; however, TSA has not yet finalized this process. According to TSA officials, the redress process will make use of TSA's existing complaint process—currently used for complaints from passengers denied boarding passes—to document complaints and provide these to TSA's Ombudsman.¹³ Complaints relating to CAPPS II will be

¹²We refer to the eight Fair Information Practices proposed in 1980 by the Organization for Economic Cooperation and Development and that were endorsed by the U.S. Department of Commerce in 1981. These practices are collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, individual participation, and accountability.

¹³The Ombudsman is the designated point of contact for TSA-related inquiries from the public.

routed through the Ombudsman to a Passenger Advocate—a position to be established within TSA for assisting individuals with CAPPs II-related concerns—who will help identify errors that may have caused a person to be identified as a false positive.¹⁴ If the passengers are not satisfied with the response received from the Passenger Advocate regarding the complaint, they will have the opportunity to appeal their case to the DHS Privacy Office.

A number of key policy issues associated with the redress process, however, still need to be resolved. These issues involve data retention, access, and correction. Current plans for data retention indicate that data on U.S. travelers and lawful permanent residents will be deleted from the system at a specified time following the completion of the passengers' itinerary. Although TSA's decision to limit the retention of data was made for privacy considerations, the short retention period might make it impossible for passengers to seek redress if they do not register complaints quickly. TSA has also not yet determined the extent of data access that will be permitted for those passengers who file a complaint. TSA officials said that passengers will not have access to any government data used to generate a passenger risk score due to national security concerns. TSA officials have also not determined to what extent, if any, passengers will be allowed to view information used by commercial data providers. Furthermore, TSA has not yet determined how the process of correcting erroneous information will work in practice. TSA documents and program officials said that it may be difficult for the Passenger Advocate to identify errors, and that it could be the passenger's responsibility to correct errors in commercial databases at their source.

To address these concerns, TSA is exploring ways to assist passengers who are consistently determined to be false positives. For example, TSA has discussed incorporating an "alert list" that would consist of passengers who coincidentally share a name with a person on a government watch list and are, therefore, continually flagged for additional screening. Although the process has not been finalized, current plans indicate that a passenger would be required to submit to an extensive background check in order to be placed on the alert list. TSA said that available remedies for all persons seeking redress will be more fully detailed in CAPPs II's privacy policy,

¹⁴Passengers who are erroneously delayed or prohibited from boarding their scheduled flights are considered false positives.

which will be published before the system achieves initial operating capability.

Other Challenges Could Affect the Successful Implementation of CAPPS II

In addition to facing developmental and operational challenges related to key areas of interest to the Congress, CAPPS II faces a number of additional challenges that may impede its success. We identified three issues that, if not adequately resolved, pose major risks to the successful development, implementation, and operation of CAPPS II. These issues are developing the international cooperation needed to obtain passenger data, managing the expansion of the program's mission beyond its original purpose, and ensuring that identity theft—in which an individual poses as and uses information of another individual—cannot be used to negate the security benefits of the system.

International Cooperation

For CAPPS II to operate fully and effectively, it needs data not only on U.S. citizens who are passengers on flights of domestic origin, but also on foreign nationals on domestic flights and on flights to the United States originating in other countries. However, obtaining international cooperation for access to these data remains a substantial challenge. The European Union, in particular, has objected to its citizens' data being used by CAPPS II, whether a citizen of a European Union country flies on a U.S. carrier or an air carrier under another country's flag. The European Union has asserted that using such data is not in compliance with its privacy directive and violates the civil liberties and privacy rights of its citizens.

DHS and European Union officials are in the process of finalizing an understanding regarding the transfer of passenger data for use by the Bureau of Customs and Border Protection. However, this understanding does not permit the passenger data to be used by TSA in the operation of CAPPS II but does allow for the data to be used for testing purposes. According to a December 16, 2003, report from the Commission of European Communities, the European Union will not be in a position to agree to the use of its citizens' passenger data for CAPPS II until internal U.S. processes have been completed and it is clear that the U.S. Congress's privacy concerns have been resolved. The Commission said that it would discuss the use of European Union citizen passenger data in a second, later round of discussions.

Expansion of Mission

Our review found that CAPPS II may be expanded beyond its original purpose and that this expansion may affect program objectives and public acceptance of the system. The primary objective of CAPPS II was to

protect the commercial aviation system from the risk of foreign terrorism by screening for high-risk or potentially high-risk passengers. However, in the August 2003 interim final Privacy Act notice for CAPPS II, TSA stated that the system would seek to identify both domestic and foreign terrorists and not just foreign terrorists as previously proposed. The August notice also stated that the system could be expanded to identify persons who are subject to outstanding federal or state arrest warrants for violent crimes and that CAPPS II could ultimately be expanded to include identifying individuals who are in the United States illegally or who have overstayed their visas.

DHS officials have said that such changes are not an expansion of the system's mission because they believe it will improve aviation security and is consistent with CAPPS II's mission. However, program officials and advocacy groups expressed concern that focusing on persons with outstanding warrants, and possibly immigration violators, could put TSA at risk of diverting attention from the program's fundamental purpose. Expanding CAPPS II's mission could also lead to an erosion of public confidence in the system, which program officials agreed is essential to the effective operation of CAPPS II. This expansion could also increase the costs of passenger screening, as well as the number of passengers erroneously identified as needing additional security attention because some of the databases that could be used to identify wanted felons have reliability concerns.

Identity Theft

Another challenge facing the successful operation of CAPPS II is the system's ability to effectively identify passengers who assume the identity of another individual, known as identity theft. TSA officials said that while they believe CAPPS II will be able to detect some instances of identity theft, they recognized that the system will not detect all instances of identity theft without implementing some type of biometric indicator, such as fingerprinting or retinal scans. TSA officials said that while CAPPS II cannot address all cases of identity theft, CAPPS II should detect situations in which a passenger submits fictitious information such as a false address. These instances would likely be detected since the data being provided would either not be validated or would be inconsistent with information in the databases used by CAPPS II. Additionally, officials said that data on identity theft may be available through credit bureaus and that in the future they expect to work with the credit bureaus to obtain such data. However, the officials acknowledge that some identity theft is difficult to spot, particularly if the identity theft is unreported or if

collusion, where someone permits his or her identity to be assumed by another person, is involved.

TSA officials said that there should not be an expectation that CAPPS II will be 100 percent accurate in identifying all cases of identity theft. Further, the officials said that CAPPS II is just one layer in the system of systems that TSA has in place to improve aviation security, and that passengers who were able to thwart CAPPS II by committing identity theft would still need to go through normal checkpoint screening and other standard security procedures. TSA officials believe that, although not fool-proof, CAPPS II represents an improvement in identity authentication over the current system.

Concluding Observations

The events of September 11, 2001, and the ongoing threat of commercial aircraft hijackings as a means of terrorist attack against the United States continue to highlight the importance of a proactive approach to effectively prescreening airline passengers. An effective prescreening system would not only expedite the screening of passengers, but would also accurately identify those passengers warranting additional security attention, including those passengers determined to have an unacceptable level of risk who would be immediately assessed by law enforcement personnel. CAPPS II, while holding the promise of providing increased benefits over the current system, faces significant challenges to its successful implementation. Uncertainties surrounding the system's future functionality and schedule alone result in the potential that the system may not meet expected requirements, may experience delayed deployment, and may incur increased costs throughout the system's development. Of the eight issues identified by the Congress related to CAPPS II, only one has been fully addressed. Additionally, concerns about mission expansion and identity theft add to the public's uncertainty about the success of CAPPS II.

Our recent report on CAPPS II made seven specific recommendations that we believe will help address these concerns and challenges. The development of plans identifying the specific functionality that will be delivered during each increment of CAPPS II and its associated milestones for completion and the expected costs for each increment would provide TSA with critical guidelines for maintaining the project's focus and achieving intended system results and milestones within budget. Furthermore, a schedule for critical security activities, a strategy for mitigating the high risk associated with system and database testing, and appropriate oversight mechanisms would enhance assurance that the

system and its data will be adequately protected from misuse. In addition to these steps, development of results-oriented performance goals and measures would help ensure that the system is operating as intended. Last, given the concerns regarding the protection of passenger data, the system cannot be fully accepted if it lacks a redress process for those who believe they are erroneously identified as an unknown or unacceptable risk.

Our recently published report highlighted each of these concerns and challenges and contained several recommendations to address them. DHS generally concurred with our findings and has agreed to address the related recommendations. By adequately addressing these recommendations, we believe DHS increases the likelihood of successfully implementing this program. In the interim, it is crucial that the Congress maintain vigilant oversight of DHS to see that these concerns and challenges are addressed.

Mr. Chairman, this concludes my statement. I would be please to answer any questions that you or other members of the Subcommittee may have at this time.

GAO Contacts and Acknowledgments

For further information on this testimony, please contact Norman J. Rabkin at (202) 512-8777 or David A. Powner on (202) 512-9286. Individuals making key contributions to this testimony include J. Michael Bollinger, Adam Hoffman, and John R. Schulze.

Appendix I: CAPPs II Developmental Increments

The following describes general areas of functionality to be completed during each of the currently planned nine developmental increments of the Computer-Assisted Passenger Prescreening System (CAPPs II).

Increment 1. System functionality established at the central processing center. By completion of increment 1, the system will be functional at the central processing center and can process passenger data and support intelligence validation using in-house data (no use of airline data). Additionally, at this increment, validation will be completed for privacy and policy enforcement tools; the exchange of, and processing with, data from multiple commercial data sources; and processing of government databases to support multiple watch-lists.

Increment 2. System functionality established to support processing airline data. At the completion of increment 2, the system is functionally and operationally able to process airline data. Additionally, the system can perform functions such as prioritizing data requests, reacting to threat level changes, and manually triggering a "rescore" for individual passengers in response to reservation changes or adjustments to the threat level.

Increment 3. This increment will provide for a functional system that will use a test simulator that will not be connected to an airline's reservation system. System hardware that includes the establishment of test and production environments will be in place and a facility capable of performing risk assessment will be established. Design and development work for system failure with a back up system and help desk infrastructure will be put in place.

Increment 4. By the completion of this increment, a back up location will be functionally and operationally able to support airlines processing application, similar to the main location. A help desk will be installed to provide assistance to airlines, authenticator, and other user personnel.

Increment 5. Enhanced intelligence interface. At the conclusion of this increment, the system will be able to receive from DHS the current threat level automatically and be able to adjust the system in response to changes in threat levels. The system will also be able to semi-automatically rescore and reclassify passengers that have already been authenticated.

Increment 6. Enhanced passenger authentication. This increment will allow the system to perform passenger authentication using multiple

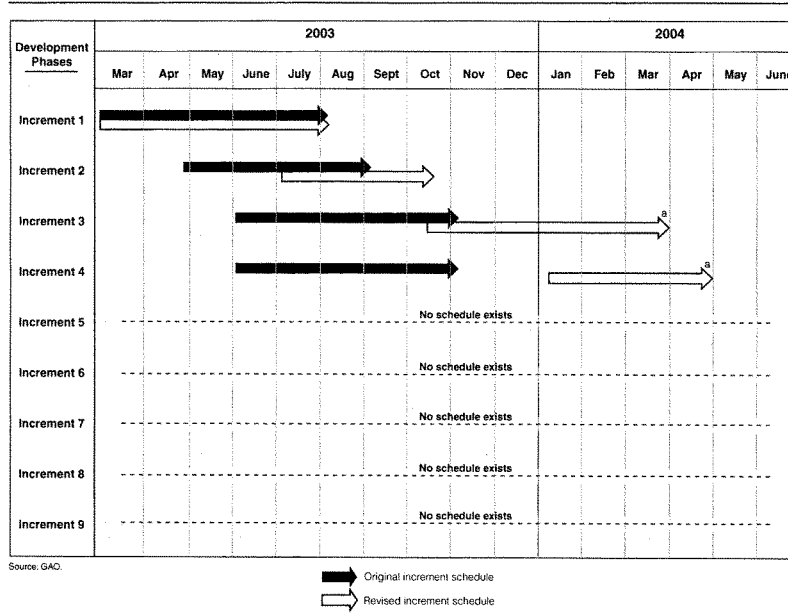
commercial data sources in the instance that little information on a passenger is available from original commercial data source.

Increment 7. Integration of other system users. By the completion of this increment, TSA Aviation Operations and law enforcement organizations will be integrated into CAPPS II, allowing multiple agencies and organizations to do manpower planning and resource allocations based on the risk level of the nation, region, airport, or specific flight.

Increment 8. Enhanced risk assessments. This increment provides for the installation of capabilities and data sources to enhance risk assessments, which will lower the number of passengers falsely identified for additional screening. This increment also provides for a direct link to the checkpoint for passenger classification, rather than having the passenger's score encoded on their boarding pass.

Increment 9. Completion of system. Increment 9 marks the completion of the system as it moves into full operation and maintenance, which will include around-the-clock support and administration of the system, database, and network, among other things.

Appendix II: Timeline for Developing CAPPS II, by Original and Revised Increment Schedule



*System functionality to be achieved at revised schedule dates will be less than originally planned.

TESTIMONY OF

PAUL ROSENZWEIG

SENIOR LEGAL RESEARCH FELLOW
CENTER FOR LEGAL AND JUDICIAL STUDIES

THE HERITAGE FOUNDATION*

214 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

SUBCOMMITTEE ON AVIATION

REGARDING

THE TRANSPORTATION SECURITY ADMINISTRATION'S
COMPUTER-ASSISTED PASSENGER PRESCREENING
SYSTEM (CAPPS II)

17 MARCH 2004

* The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2003, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2003 income came from the following sources: Individuals 52%; Foundations 19%; Corporations 8%; Investment Income 18%; Publication Sales and Other 3%. The top five corporate givers provided The Heritage Foundation with 5% of its 2003 income. The national accounting firm of Deloitte & Touche audits the Heritage Foundation's books annually. A list of major donors is available from The Heritage Foundation upon request. Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to testify before you today on the challenge of maintaining the balance between security and constitutionally protected freedoms inherent in responding to the threat of terror, in the particular context of the Transportation Security Administration's (TSA's) proposed Computer-Assisted Passenger Prescreening System, known as CAPPs II.

For the record, I am a Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation, a nonpartisan research and educational organization. I am also an Adjunct Professor of Law at George Mason University where I teach Criminal Procedure and an advanced seminar on White Collar and Corporate Crime. I am a graduate of the University of Chicago Law School and a former law clerk to Judge R. Lanier Anderson of the U.S. Court of Appeals for the Eleventh Circuit. For much of the past 15 years I have served as a prosecutor in the Department of Justice and elsewhere, prosecuting white-collar offenses. During the two years immediately prior to joining The Heritage Foundation, I was in private practice representing principally white-collar criminal defendants. I have been a Senior Fellow at The Heritage Foundation since April 2002.

I note, as well, (with some degree of pride) that I formerly served on the staff of this Committee as Counsel (Investigations) under the Chairmanship of the Honorable Bud Shuster. So this is, in a way, a homecoming for me and I am pleased to be back in this room.

My perspective on the question before you is that of a lawyer and a prosecutor with a law enforcement background, not that of a technologist or an intelligence officer/analyst. I should hasten to add that much of my testimony today is based upon a series of papers I have written (or co-authored with my colleagues James Carafano and Ha Nguyen) on various aspects of this topic and testimony I have given before other bodies in Congress, all of which are available at The Heritage Foundation website (www.heritage.org). A substantial portion of my testimony today are derived from a forthcoming law review article entitled "Civil Liberty and the Response to Terrorism" which will be published in the *Duquesne Law Review* Spring 2004 issue.¹ For any who might have read portions of my earlier work, I apologize for the familiarity that will attend this testimony. Repeating myself does have the virtue of maintaining consistency -- I can only hope that any familiarity with my earlier work on the subject does not breed contempt.

* * * * *

The civil liberty/national security question is *the* single most significant domestic legal issue facing America today, bar none. And, as is reflected in my testimony today, in my judgment one of the most important components of a responsible governmental policy addressing this difficult question will be the sustained, thoughtful, non-partisan attention of America's elected leaders in Congress. Nothing is more likely, in my judgment, to allow

¹ See Paul Rosenzweig, "Civil Liberty and the Response to Terrorism," 42 *Duq. L. Rev.* ____ (2004) (forthcoming)

America to find the appropriate balance than your engagement in this issue. What I would like to do today is assist your consideration of this question by sharing with you some general principles regarding the nature of the threat and then nature of the liberty interest at stake, which underlie my analysis of the CAPPs II program. Then I'd like to apply those principles to the concrete issues raised by the CAPPs II program. Finally, I will offer some thoughts on aspects of CAPPs II where innovative technological solutions may answer some of the challenges the program confronts and ways in which the technological programs that underlie CAPPs II can aid security even if CAPPs II is not implemented in its current proposed configuration.

I. The Threat of Terrorism – Type I and Type II Errors

The full extent of the terrorist threat to America cannot be fully known. Consider, as an example, one domestic aspect of that threat—an effort to determine precisely how many al-Qaeda operatives are in the United States at this time and to identify those who may seek to fly on domestic airplanes in the future. This is the problem to which CAPPs II is directed.

Terrorism remains a potent threat to international security – as the events of last week all too tragically demonstrate. The list of terrorist targets now includes Madrid, Bali, Baghdad, Najaf, Karachi, Istanbul, Mombassa, Jerusalem, Riyadh, Casablanca and of course New York and Washington. The attacks in Spain demonstrate that we cannot return to the “law enforcement” mindset for handling terrorism that existed prior to September 11. Terrorism is not a crime, to be prosecuted after the fact, like murder. We have, in recent months, been tempted to forget this fact – but we cannot.

Let's examine the scope of the problem: The U.S. State Department has a list of over 100,000 names worldwide of suspected terrorists or people with contact with terrorists.² Before their camps in Afghanistan were shut down, Al Qaeda trained at least 70,000 people and possibly tens of thousands more.³ Al Qaeda linked Jemaah Islamiyah in Indonesia is estimated to have 3,000 members across Southeast Asia and is still growing larger.⁴ Although the estimates of the number of al-Qaeda terrorists in the United States have varied since the initial attack on September 11, the figure provided by the government in supposedly confidential briefings to policymakers is 5,000.⁵ This 5,000-person estimate may include many who are engaged in fundraising for terrorist organizations and others who were trained in some fashion to engage in jihad, whether or not they are actively engaged in a terrorist cell at this time. But these and other publicly available statistics support two conclusions: (1) no one can say with much certainty how many terrorists are living in the

² Lichtblau, Eric. “Administration Creates Center for Master Terror ‘Watch List.’” *New York Times*, Sept. 17, 2003.

³ On an interview on NBC’s “Meet the Press,” U.S. Senator Bob Graham was quoted as saying, “...al-Qaeda has trained between 70,000 and 120,000 persons in the skills and arts of terrorism.” *Meet the Press* (July 13, 2003).

⁴ Hunt, Terence. “Bush shows resolve by visiting Bali.” *Chicago Sun-Times*, Oct. 22, 2003, p. 36.

⁵ Bill Gertz, “5,000 in U.S. Suspected of Ties to al Qaeda.” *The Washington Times*, July 11, 2002.

United States, and (2) many of those who are in the United States may seek to fly on domestic airlines in the foreseeable future.

And, the scope of the problem is enormous. These comparatively few potential terrorists are hidden in a sea of travelers. For 2003 there were over 8.5 million domestic airplane departures, and more than 1.2 million international departures.⁶ These planes carried over 552 million domestic and more than 123 million international passengers⁷ – each of whom requires some form of individual screening.

These statistics illustrate the difficulty of the problem. The danger to America posed by terrorists arises from the new and unique nature of potential acts of war. Virtually every terrorism expert in and out of government believes there is a significant risk of another attack – and Madrid proves that point. Unlike during the Cold War, the threat of such an attack is asymmetric. In the Cold War era, U.S. analysts assessed Soviet capabilities, thinking that their limitations bounded the nature of the threat the Soviets posed. Because of the terrorists' skillful use of low-tech capabilities (e.g. box cutters) their capacity for harm is essentially limitless. The United States therefore faces the far more difficult task of discerning their intentions and thwarting them. Where the Soviets created "things" that could be observed, the terrorists create only transactions and events that can be sifted from the noise of everyday activity only with great difficulty. It is a problem of unprecedented scope, and one whose solution is imperative if American lives are to be saved.

As should be clear from the outline of the scope of the problem, the suppression of terrorism will not be accomplished by military means alone. Rather, effective law enforcement and/or intelligence gathering activity are the key to avoiding new terrorist acts. Recent history supports this conclusion.⁸ In fact, police have arrested more terrorists than military operations have captured or killed. Police in more than 100 countries have arrested more than 3000 Al Qaeda linked suspects,⁹ while the military captured some 650 enemy combatants.¹⁰ Equally important, it is policing of a different form – preventative rather than reactive – since there is less value in punishing terrorists after the fact when, in some instances, they are willing to perish in the attack.

The foregoing understanding of the nature of the threat from terrorism helps to explain why the traditional law enforcement paradigm needs to be modified (or, in some instances, discarded) in the context of terrorism investigations. The traditional law enforcement model is highly protective of civil liberty in preference to physical security. All lawyers have heard one or another form of the maxim that "it is better that 10 guilty go free

⁶ Bureau of Transportation Statistics, Domestic Segment – Departures (available at <http://www.transtats.bts.gov/DataIndex.asp>); *id.* International Segment – Departures.

⁷ *Id.* Domestic Market – Passengers; *id.* International Market – Passengers.

⁸ See, e.g. Dana Dillon, *War on Terrorism in Southeast Asia: Developing Law Enforcement*, Backgrounder No. 1720 (Heritage Foundation Jan. 22, 2004).

⁹ Slevin, Peter. "U.S. Pledges Not to Torture Terror Suspects." *The Washington Post*, June 27, 2003, p. A01

¹⁰ Taylor, Francis. "Transcript: State Dept Official Says War Against Terrorism Continues." June 9, 2003, available at <http://usembassy.state.gov/tokyo/www/wh20030611a6.html>

than that 1 innocent be mistakenly punished.”¹¹ This embodies a fundamentally moral judgment that when it comes to enforcing criminal law American society, in effect, prefers to have many more Type II errors (false negatives) than it does Type I errors (false positives).¹² That preference arises from two interrelated grounds: one is the historical distrust of government that animates many critics of CAPPs II. But the other is, at least implicitly, a comparative valuation of the social costs attending the two types of error. We value liberty sufficiently highly that we see a great cost in any Type I error. And, though we realize that Type II errors free the guilty to return to the general population, thereby imposing additional social costs on society, we have a common sense understanding that those costs, while significant, are not so substantial that they threaten large numbers of citizens or core structural aspects of the American polity.

The post-September 11 world changes this calculus in two ways. First, and most obviously, it changes is the cost of the Type II errors. Whatever the costs of freeing John Gotti or John Muhammed might be, they are substantially less than the potentially horrific costs of failing to stop the next al-Qaeda assault. Thus, the theoretical rights-protective construct under which our law enforcement system operates must, of necessity, be modified to meet the new reality. We simply cannot afford a rule that “better 10 terrorists go free than that 1 innocent be mistakenly screened or delayed.”

Second, and less obviously, it changes the nature of the Type I errors that must be considered. In the traditional law enforcement paradigm the liberty interests at stake is personal liberty – that is, freedom from the unjustified application of governmental force. We have as a model, the concept of an arrest, the seizure of physical evidence, or the search of a tangible place. As we move into the information age, and deploy new technology to assist in tracking terrorists, that model is no longer wholly valid.

Rather, we now add related, but distinct conception of liberty to the equation – the liberty that comes from anonymity.¹³ Anonymity is a different, and possibly weaker, form of liberty: The American understanding of liberty interests necessarily acknowledges that the personal data of those who have not committed any criminal offense can be collected for legitimate governmental purposes. Typically, outside the criminal context, such collection is done in the aggregate and under a general promise that uniquely identifying individual information will not be disclosed. Think, for example, of the Census data collected in the aggregate and never disclosed, or of the IRS tax data collected on an individual basis,

¹¹ *E.g. Furman v. Georgia*, 408 U.S. 238, 367 n. 158 (1972) (Marshall, J., concurring). The aphorism has its source in 4 Blackstone, Commentaries, ch. 27 at 358 (Wait & Co. 1907).

¹² “In a criminal case ... we do not view the social disutility of convicting an innocent man as equivalent to the disutility of acquitting someone who is guilty [T]he reasonable doubt standard is] bottomed on a fundamental value determination of our society that it is far worse to convict an innocent man than to let a guilty man go free.” *In re Winship*, 397 U.S. 357, 372 (1970) (Harlan, J., concurring).

¹³ See Phillip Kurland, “The private I,” *The University of Chicago Magazine*, Autumn 1976, p. 8 (characterizing three facets of privacy, broadly characterized as anonymity, secrecy, and autonomy), quoted in *Whalen v. Roe*, 429 U.S. 589, 599 n.24 (1977).

reported publicly in the aggregate, and only disclosed outside of the IRS with the approval of a federal judge based upon a showing of need.¹⁴

What these examples demonstrate is not so much that our conception of liberty is based upon absolute privacy expectations, but rather that government impingement on our liberty will occur only with good cause. In the context of a criminal or terror investigation, we expect that the spotlight of scrutiny will not turn upon us individually without some very good reason.

This conception of the liberty interest at stake (the interest that will be lost when Type I errors occur) also emphasizes one other point about privacy – in many ways the implementation of new laws and systems to combat terror are not an unalloyed diminution of privacy. Rather the laws and practices can substitute one privacy intrusion (for example, a search of electronic data about an individual) for another privacy intrusion (the physical intrusiveness of body searches at airports).

Let me record, here, an anecdote that illustrates the point – I’ve obscured the identifying details a bit to protect my traveling companions’ anonymity, but I assure you the incident is true: Recently I was traveling through a small airport in the West that was quite a distance from any border and not an origination point (or arrival point) for any international travel. Thus, the airport was a “low risk” for terrorist infiltration. One of my traveling companions was a female federal judge of adult years – completely outside the profile for a terrorist. Nonetheless, the TSA complement, as part of its routine searches, selected her for a complete screen of her luggage. They proceeded to publicly examine all of her clothing, including the dirty laundry she had accumulated at the conference we had attended, literally displaying her lingerie to anyone who cared to view it. My companion was mortified and hastily urged all of us to go on to the gate and not wait for her, as we had been. I have absolutely no doubt that at that moment, if she had been asked, she would have gladly traded a small amount of electronic privacy that would have verified her identity as a federal judge for the significant physical intrusion she suffered.

But this means that legal analysts cannot make broad value judgments – each person weighs the utility of their own privacy by a different metric. For many Americans, the price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy – for others the opposite result might hold. This suggests little in resolving the tension, save that it cautions against allowing the tension to be resolved by unrepresentative institutions like the courts and in favor of allowing more representative institutions, like the Congress, to do their best at evaluating the multi-variable privacy preferences of the population. I would urge you not, therefore, to be categorical in your condemnation of any form of privacy intrusion – for you are not eliminating all intrusions, merely trading one form for another.

Finally, it bears noting that not all solutions necessarily trade off Type I and Type II errors, and certainly not in equal measure. Some novel approaches to combating terrorism

¹⁴ *E.g.* 26 U.S.C. § 7213 (prohibiting disclosure of tax information except as authorized for criminal or civil investigations).

might, through technology, actually reduce the incidence of both types of error.¹⁵ More commonly, we will alter both values but the comparative changes will be the important factor. Where many critics of governmental initiatives go wrong is, it seems to me, in their absolutism – they refuse to admit of the possibility that we might need to accept an increase in the number of a limited sort of Type I errors. But that simply cannot be right – liberty is not an absolute value, it depends on security (both personal and national) for its exercise. As Thomas Powers has written: “In a liberal republic, liberty presupposes security; the point of security is liberty.”¹⁶ The growth in danger from Type II errors necessitates altering our tolerance for Type I errors. More fundamentally, our goal should be to minimize both sorts of errors.

II. CAPPS II

One common critique offered by skeptics of new initiatives to combat terrorism is the concern that advances in information technology will unreasonably erode the privacy and anonymity to which American citizens are entitled. They fear, in effect, the creation of an “electronic dossier” on every American. Attention to this issue has particularly focused on TSA’s proposal to use an enhanced information technology program to screen airplane passengers. That program, known as CAPPS II, would effectively conduct a computerized screen of every passenger to assess his or her potential threat as a terrorist.

Since September 11th, the aviation industry has undergone many changes to strengthen airport security. The TSA was created and placed in charge of passenger and baggage screeners (who are now federal employees). It has been using explosives detection systems on 90 percent of checked baggage and substantially expanded the Federal Air Marshal Service. However, little has been done to determine whether a person seeking to board an aircraft belongs to a terrorist organization or otherwise poses a threat. In order to meet this objective, the Transportation Security Administration is developing the Computer Assisted Passenger Prescreening System II (CAPPS II).

Most of the changes made in airport security have focused on looking for potential weapons (better examination of luggage, more alert screeners) and creating obstacles to the use of a weapon on an aircraft (reinforced cockpit doors, armed pilots, etc). A computer-aided system would improve the TSA’s ability to assess the risk a passenger may pose to air safety.

A Bit Of History – CAPPS I: The current, limited CAPPS I system was first deployed in 1996 by Northwest Airlines. Other airlines began to use CAPPS I in 1998, as recommended by the White House Commission on Aviation Safety and Security (also known as the Gore Commission).¹⁷ In 1999, responding to public criticism, the FAA limited the use of CAPPS I – using it only to determine risk assessments for checked luggage screening. In other words, between 1999 and September 2001 CAPPS I information was not used as a basis for subjecting passengers to personal searches and questioning – only for

¹⁵ See K. A. Taipale, “Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data,” 5 Colum. Sci. & Tech. L. Rev. 2, 31 (December 2003) (arguing for utility of strong audit technology) (available at <http://www.stlr.org/cite.cgi?volume=5&article=2>).

¹⁶ Thomas Powers, “Can We Be Secure and Free?” *The Public Interest* (Spring 2003)

¹⁷ See White House Commission on Aviation Safety and Security (Feb. 12, 1997) (available at <http://www.airportnet.org/depts/regulatory/gorefina.htm>).

screening checked bags. As a consequence even if CAPPS I flagged a high-risk passenger he could not be singled out for more intensive searches.

After September 11 CAPPS I returned to its original conception and is now again used to screen all passengers along with their carry-on and checked luggage. However, the criteria used to select passengers, such as last-minute reservations, cash payment, and short trips are over inclusive. This is a very crude form of pattern-recognition analysis. So crude that it can flag up to 50% of passengers in some instances, mainly in short haul markets.¹⁸ These criteria are also widely known and thus readily avoided by any concerted terrorist effort. Nor does CAPPS I attempt to determine whether or not the federal government has information that may connect a specific perspective passenger with terrorism or criminal activity that may indicate they are a threat to the flight. And it is costly – I've heard informal estimates as high as \$150 million per year for domestic airlines to operate the system. As a result, we are wasting resources: it's likely that if Osama bin Laden tried to board a plane today CAPPS would not identify him for arrest or further inspection.¹⁹

Changing The System -- CAPPS II: The TSA believes that screening what a passenger is carrying is only part of the equation and is developing CAPPS II as a successor to CAPPS I in order to determine whether the individual poses a threat to aviation security. CAPPS II will use government intelligence and law enforcement information in order to assign risk levels to passengers based on real information not arbitrary models. The TSA will then be able to devote more of its resources to those with a higher score (indicating they pose a greater risk), than those deemed to be a lesser concern (although some degree of randomness will need to be retained).

In January 2003, TSA released a Privacy Act notice for CAPPS II, the successor to CAPPS I.²⁰ Since then, many critics have raised substantial concerns. Some thought that CAPPS II, as originally proposed, was too broad in scope and could infringe on passengers' privacy. Others were concerned that the government should not rely on potentially flawed commercial data to prevent individuals from traveling by air. Some asserted that the use of knowledge discovery technologies on a wide variety of personal data could pose privacy and civil liberty violations. Finally, many wondered if individuals would be able to challenge their score.

¹⁸ See Robert W. Poole, Jr. & George Passatino, "A Risk-Based Airport Security Policy" Reason Public Policy Institute at 11 (May 2003).

¹⁹ It has been reported that the CAPPS I system was partially effective, flagging nine of the 19 September 11 terrorists for additional screening. See National Commission on Terrorist Attacks Upon the United States, "The Aviation Security System and the 9/11 Attacks: Staff Statement No. 3" (Jan. 27, 2004) (available at http://www.9-11commission.gov/hearings/hearing7/staff_statement_3.pdf); see also Sara Goo and Dan Eggen, "9/11 Hijackers Used Mace and Knives, Panel Reports," Wa. Post at A1 (Jan. 28, 2004) (summarizing report). To the extent that is true it emphasizes both that some form of screening can be effective, that the limitation to bag-only screening was unwise, and that however effective electronic screening might be, the human element will always be a factor in insuring the success of any system.

²⁰ See 68 Fed. Reg. 2101 (Jan. 15, 2003).

In August 2003, TSA made available an Interim Final Privacy Notice on CAPPS II, which includes substantial modifications to the initial proposal based on many of the concerns voiced in response to the first Privacy Notice.²¹

Under the Interim Notice, TSA will not keep any significant amount of information after the completion of a passenger's itinerary. Furthermore, TSA anticipates that it will delete all records of travel for U.S. citizens and lawful permanent residents a certain number of days after the safe completion of the passenger's travels (7 days is the current anticipation). TSA has also committed to developing a mechanism by which a passenger targeted for more thorough screening can seek to set the record straight if they think they have been identified in error.

More importantly, the CAPPS II system has addressed privacy concerns by severely limiting the types of private information collected and the way in which commercial data will be examined. The proposed CAPPS II system will access only a "passenger name record" (PNR), which will include information collected at the time the passenger makes the reservations, prior to the flight. Selected PNR information (including name, address, date of birth, and telephone number) will be transmitted to commercial data providers for the sole purpose of authenticating the passenger's identity. This process is similar to the credit card application procedure used to check for fraudulent information.

The way this works is relatively straightforward, and is in common use today in the commercial world. A requesting party, whether TSA or a commercial user, submits information (*e.g.* name, address, phone number and date of birth) about an individual. That identification information is then compared to information held in numerous commercial databases. A numeric score, reflecting the confidence with which an identity is authenticated is then generated for each of the four pieces of information – that score itself is based upon both the quality of the databases queried and the frequency with which matches within the database are found. The scores for each independent data field are then combined for a cumulative score. Commercial data providers will then transmit back to TSA a numeric score indicating the degree of match between commercial data and TSA data, giving TSA a good idea if the person is who they say they are.²² No commercial data will be retained by the TSA and the commercial companies will retain no travel data.

After the authentication phase, the CAPPS II system will conduct a further risk assessment by comparing that identification information to intelligence and law enforcement data. The thresholds for action can be adjusted generically based upon existing external threat intelligence. If we have information that some form of attack is imminent, the threshold score for enhanced screening can be lowered – and vice versa. Passengers whose identity is confirmed with a high degree of confidence and have no matches with intelligence or law enforcement data will be less likely to receive additional scrutiny, whereas those on the opposite end of the spectrum will likely be searched more thoroughly or arrested as

²¹ See 68 Fed. Reg. 45265 (Aug. 1, 2003).

²² Absolute certainty of identification is impossible. In practice, all identification will be expressed as a "confidence interval" reflecting an estimate of the degree of certainty in an identification. For most travelers, this confidence interval will be quite high. For a few, who will be subject to greater screening, it will not.

appropriate. This will allow TSA to focus its prevention resources on those passengers who, through a qualitative analysis, are determined to more dangerous.

Assessing The Risks of Type I and Type II Errors: The CAPPS II program poses some interesting and challenging problems in adapting the law to new technology and the realities of new technology to the law. First, if CAPPS II is to be effective its hallmark will be the idea that some form of “result” will necessarily be immediately available to TSA screeners on a “real-time” basis so that they can make near-instantaneous decisions regarding whom to screen or not screen prior to allowing passengers to board the aircraft. If CAPPS II were designed so that detailed personal information on each passenger were transmitted to every TSA screener, all would agree that the architecture of the system did not adequately protect individual privacy. The analysis passed by the CAPPS II system to TSA employees at the airport must be (and under current plans, will be) limited to a reported color code – red, yellow or green – and should not generally identify the basis for the assignment of the code.

Thus, CAPPS II proposes to precisely reverse the privacy protection equation being developed in other contexts. To protect privacy, other information technology program disaggregate analysis from identity by making the data available to the analyst while concealing the identity of the subject of the inquiry unless and until disclosure is warranted. In the reverse of this paradigm, CAPPS II will disclose the identity of the potential threat (through a red/yellow/green system displayed to the screener, warning of a particular individual) but will conceal from the screener the data underlying the analysis – at least until such time as a determination is made that the two pieces of information should be combined. The privacy protection built into CAPPS II is therefore the mirror image of the more common system. It is by no means clear which method of protecting privacy is *ex ante* preferable – but it is clear that the two systems operate differently and if we are to have any sort of CAPPS II system at all, it can only have privacy protections of the second kind.

To reiterate a point made earlier, CAPPS II is not necessarily a decrease in privacy. Rather, it requires trade-offs in different types of privacy. It substitutes one privacy intrusion (into electronic data) for another privacy intrusion (the physical intrusiveness of body searches at airports). It will allow us to target screening resources, while actually *reducing* the number of intrusive searches: Currently 14% of the traveling public are subject to some form of secondary screening. CAPPS II will likely reduce that to 4% for additional screening.²³ CAPPS II may also have the salutary effect of reducing the need for random searches and eliminate the temptation for screeners to use objectionable characteristics of race, religion, or national origin as a proxy for threat indicators.²⁴ For many Americans, the

²³ See Transcript of Media Roundtable with DHS Under Secretary Asa Hutchinson (Feb. 12, 2004) (available at www.tsa.gov).

²⁴ Some purely random searches will need to be retained in order to maintain the integrity of the inspection system and defeat so-called “Carnival Booth” attacks (named after a student algorithm proposing a method of defeating CAPPS). Adding a random factor to the inspection regime answers the problem. See Samidh Chakrabati & Aaron Strauss, “Carnival Booth: An Algorithm for Defeating the Computer-assisted Passenger Screening,” (available at <http://www.swiss.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>) (describing program); Taipale, “Data Mining and Domestic Security,” at n. 285 (explaining how addition of random screening guards against such attacks).

price of a little less electronic privacy might not be too great if it resulted in a little more physical privacy, fewer random searches, and a reduction in invidious racial profiling.

Finally, the subject matter of the CAPPs II system calls for heightened sensitivity to the potential for an infringement on protected constitutional liberties. While the Constitution affords no additional protection to information that an individual has made available to other individuals or institutions and while CAPPs II will not directly affect personal physical liberty, which lies at the core of constitutional protections, CAPPs II does implicate at least one fundamental liberty interest guaranteed by the Constitution. Since the 1960s the Supreme Court has recognized a fundamental right to travel²⁵ – indeed, one might reasonably say that one purpose of the Federal union was to insure the freedom of commerce and travel within the United States.

Thus, there is a risk that a poorly designed system will unreasonably impinge upon a fundamental constitutional liberty. The risk of such impingement should not result in abandonment of the program – especially not in light of the potentially disastrous consequences of Type II error if there is another terrorist attack in the United States. However, we will need stringent oversight to provide the requisite safeguards for minimizing infringements of civil liberty in the first instance and correcting them as expeditiously as possible.

CAPPs II is therefore a paradigm for answering the question of whether or not we can conceive of a suitable oversight mechanism that would appropriately constrain executive authority while allowing its application to circumstances we consider necessary. In my view, the use of CAPPs II should be subject to significant Congressional oversight, including spot checks (in a classified means, if necessary) to insure that the CAPPs II methodology is not being misused. Though the details would need, of course, to be further developed, the outline of such an oversight system might include some or all of the following components:

- CAPPs II should be constructed to include an audit trail so that its use and/or abuse can be reviewed;
- It should not be expanded beyond its current use in identifying suspected terrorists and threats to national security – it should not be used as a means, for example, of identifying drug couriers or deadbeat dads.²⁶ Thus, the pending proposal to screen for outstanding criminal warrants should be modified;
- The program should sunset after a fixed period of time, thereby ensuring adequate Congressional review;
- CAPPs II should have significant civil and criminal penalties for abuse;
- The “algorithms” used to screen for potential danger must, necessarily, be maintained in secret, as there disclosure would frustrate the purpose of CAPPs II. They must, however, also be subject to appropriate congressional

²⁵ *Shapiro v. Thompson*, 398 U.S. 618 (1969)

²⁶ Cf. William Stuntz, “Local Policing After the Terror,” 111 Yale L. J. 2137, 2183-84 (2002) (use of expanded surveillance authority to prosecute only terrorists and other serious offenses).

scrutiny in a classified setting and, if necessary, independent (possibly classified) technical scrutiny;

- An individual listed for additional screening or prohibited from flying should be entitled to know the basis for his or her listing and should have a mechanism for challenging the listing before a neutral arbiter or tribunal. To the extent practicable the review should be as prompt as possible;
- Because commercial databases may be error-ridden, no American should be totally denied a right to travel (i.e. red-carded) and subject to likely arrest as a suspected terrorist solely on the basis of public, commercial data. An indication of threat sufficient to warrant denial of that right should (except in extraordinarily compelling circumstances) be based only upon significant intelligence from non-commercial sources.
- The CAPPs II system should be designed so that the No-Fly/Red Card designation, though initially made as the product of a computer algorithm, is never transmitted to the “retail” TSA screening system until it has been reviewed and approved by an official of sufficiently high authority within TSA to insure accountability for the system.²⁷ Nor is there any reason for the underlying data ever to be transmitted to the TSA screener.

To a large degree, the pending CAPPs II proposal is already structured to meet many of these criteria. For example, the software platform under which CAPPs II will operate already incorporates strong audit trail systems to uncover abuse and a use-permission system that limits the potential. The software, known as Radiant Trust, is derived from legacy technology certified by the National Security Agency. It may not be perfect, but it certainly is the best we can produce today. Similarly, current plans are to never impose anything more than enhanced screening on passengers on the basis of commercial data – only governmental data will be used to list a passenger as a “No Fly” risk.

Thoughtful critics have identified at least three potentially significant problems in the current proposed system – the possibility of mission creep, the need for a redress system and the possibility that it will be thwarted by identity theft. Let me address each of these.

Regarding mission creep, I remain a friendly critic of TSA. Given my understanding of the nature of the balance of harms – that is, the nature of the Type I and Type II errors involved – I am one who is willing to alter the scope of permitted government powers, to combat the threat of terror. The closely related point, of course, is that we must guard against “mission creep.” Since the justification for altering the traditional assessment of comparative risks is in part based upon the altered nature of the terrorist threat, we cannot alter that assessment and then apply it in the traditional contexts.²⁸ But this problem is

²⁷ This would mirror the view of the European Union which styles it as a “right” to have human checking of adverse automated decisions. The EU Directives may be found at <http://www.dataprivacy.ie/6aii-2.htm#15>.

²⁸ See Paul Rosenzweig and Michael Scardaville, *The Need to Protect Civil Liberties While Combating Terrorism: Legal Principles and the Total Information Awareness Program*, Legal Memorandum No. 6, at 10-11 (The Heritage Foundation February 2003); (arguing for use of new technology only to combat terrorism); Stuntz, “Local Policing After the Terror,” 111 Yale L. J. at 2183-84 (arguing for use of information sharing only to combat most serious offenses).

soluble. Congress can and should implement policy limitations regarding this aspect of the CAPPS II implementation. I think that “slippery slope” arguments are basically an appeal to abandoned rationality – we can and should draw rational lines with the expectation that we can adhere to them.

The concerns with regard to redress are also well taken – though not without solution. At this juncture, all we have is a commitment for such a system. Unlike some critics, I certainly anticipate that TSA will honor that commitment and provide a viable redress system – and it is no basis for rejecting a proposal that it has yet to be fully fleshed out. Any system for redress must meet the following criteria:

- It must be administratively nimble and quick, so that false positives who are delayed in travel are corrected as rapidly as possible;
- It must be supple enough to ensure against repetition – that is, the system must accommodate correction in a way that allows an individual to travel in the future without being again mistakenly singled out; and
- There must be independent review of any adverse resolution where the administrative process denies correction.

But these are not impossible criteria. They can be readily met.²⁹ To be sure, the Congress should oversee the process, but it, too, can be accomplished.³⁰

The identity theft problem is somewhat more intractable.³¹ Thus, while the technology will allow the resolution of an identity – that is determining whether the identity is a false, created one or not – it cannot resolve the theft of a true identity.³² Given the limited amount of information being requested in the PNR (name, address, date of birth, and telephone number) it is possible that individuals could pose as people other than themselves readily. The only ways to enhance CAPPS II to fight this prospect are to strengthen it -- by collecting additional information about an individual; to return additional information (for example, gender, height, weight and hair color) to the TSA screener so that the screener could confirm the identity of the individual before him; or by requiring travelers

²⁹ I outlined in more detail an appropriate system of administrative and judicial review for false positives in Paul Rosenzweig, “Proposals for Implementing the Terrorism Information Awareness System,” Legal Memorandum No. 8 (The Heritage Foundation August 2003).

³⁰ One challenge for designing such a process will be the competing impulses of critics who both want CAPPS II to purge individual information rapidly and who want a redress system that must, fundamentally, conduct a review of the individual information. Thus, the presentation of a challenge to a screening decision will need to trigger the retention of data about the individual until the challenge is resolved.

³¹ Identity theft – stealing a real identity – should be distinguished from identity fraud – creating a new, fraudulent identity. Identity fraud is a far less difficult problem and is, essentially, solved.

³² See GAO, Aviation Security: Computer Assisted Passenger Prescreening System Faces Significant Implementation Challenges at 29-30 (GAO-04-385) (Feb. 2004) (available at <http://www.gao.gov/new.items/d04385.pdf>).

to use some verified token or identification with clearance incorporated in it.³³ These are neither technologically easy nor necessarily desirable results – yet the conundrum of identity theft must be solved if CAPPs II is to prove at all useful.³⁴

The current architecture of the system offers the best prospect for combating the identity theft problem. CAPPs II will rely on the same structure that commercial users employ using their “best practices.” And those commercial users have a significant financial incentive to insuring that the algorithms prevent identity theft. We are thus doing the wise thing in harnessing the discipline of the market place as a means of enabling improvement and change. Also, the use of readily available commercial systems weakens, somewhat, any privacy objection – it is at least a little odd to say that the same system we use daily to verify a credit card application somehow becomes an horrific intrusion when it is used to identify potential terrorist risks.

Of equal significance, the criticism that the CAPPs II system is subject to potential defeat through identity theft misses one of the most significant and important points about enhanced security. We know that *no* security system is perfect – thus, instead of relying on a single system of security without backup (a “brittle” system) we prefer to use layered security systems of as many different forms as reasonable, so that the overall security system is flexible – it bends but it doesn’t break. The “reasonableness” of a new system depends, of course, on its costs, the level of its intrusiveness, and the ease or difficulty with which it may be defeated. But the mere possibility of defeat is not enough to warrant rejections – and given what we know of how identity verification works in the commercial world (it is highly successful, for example, in Las Vegas identifying gambling cheaters),³⁵ there is every reason to anticipate that CAPPs II will meet the cost-benefit threshold of utility.

Which brings us to the final question of effectiveness. Of course, before full deployment, CAPPs II needs to demonstrate that it can work.³⁶ It holds great promise – but

³³ See K. A. Taipale, “Identification Systems and Domestic Security: Who’s Who in Whoville,” Potomac Institute for Policy Studies (Jan. 28, 2003) (available at <http://www.stilwell.org/presentations/CAS-IDsystems-012804.pdf>)

³⁴ One could also take steps to harden identification cards to ensure they are less readily falsifiable and more certainly government products. See Markle Foundation, “Task Force on National Security in the Information Age,” App. A “Reliable Identification for Homeland Protection and Collateral Gains” (Dec. 2003) (recommending hardened drivers license identification). Such hardening will not, however, be of great utility unless we also strengthen the authentication process to insure that those seeking identification are who they say they are. Colorado’s recent adoption of a biometric face identification mechanism offers some promise of a technological solution to that question. See State of Colorado Deploys Facial Recognition Technology to Fight Identity Theft (Digimarc 2003) (reporting detection of 20 attempted frauds per month through facial recognition technology).

³⁵ See Don Clark, “Entrepreneur Offers Solution for Security-Privacy Clash,” Wall St. J. at B1 (March 11, 2004).

³⁶ Thus, I agree with the GAO that CAPPs II must prove its utility. See GAO, “Aviation Security” at 13-20. What I find problematic is GAO’s critique that the absence of such proof is evidence of problems within the program. Of course CAPPs II needs to be tested and refined – and it should be. See James Jay Carafano, Paul Rosenzweig & Ha Nuygen, “Passenger Screening Program is Vital – And Vital to Get Right,” Web Memo No. 428 (The Heritage Foundation, Feb. 18, 2004)

promise is far different from reality. Thus, the ultimate efficacy of the technology developed is a vital antecedent question. If the technology proves not to work—if, for example, it produces 95 percent false positives in a test environment—than all questions of implementation may be moot. For no one favors deploying a new technology—especially one that impinges on liberty—if it is ineffective. Thus, CAPPs II must be thoroughly tested. Conversely, we are unwise to reject it before knowing whether the effectiveness problem can be solved.

Some critics are skeptical that CAPPs II can ever work, characterizing it as the search for a “silver bullet” that cannot function because of Bayesian probability problems.³⁷ That broad statistical criticism is rejected by researchers in the field who believe that because of the high correlation of data variables that are indicative of terrorist activity, a sufficient number of variables can be used in any model to create relational inferences and substantially reduce the incidence of false positives.³⁸ And, in other environments, enhanced technology allowing the correlation of disparate databases and information has proven to have potentially significant positive uses. American troops in Iraq, for example, use the same sorts of link and pattern analysis, prediction algorithms and enhanced database technology that would form a part of CAPPs II to successfully track the guerrilla insurgency.³⁹

It is also important to realize that there may be potentially divergent definitions of “effectiveness.” Such a definition requires *both* an evaluation of the consequences of a false positive *and* an evaluation of the consequences of failing to implement the technology. If the consequences of a false positive are relatively modest (e.g. enhanced screening), and if the mechanisms to correct false positives are robust (as recommended herein), then we might accept a higher false positive rate precisely because the consequences of failing to use CAPPs II technology (if it proves effective) could be so catastrophic. In other words, we might accept 1,000 false positives if the only consequence is heightened surveillance and the benefit gained is a 50 percent chance of preventing the next terrorist flight attack. The vital

(available at <http://www.heritage.org/Research/HomelandDefense/wm428.cfm>). But to critique a developmental program for incomplete testing puts the cart before the horse.

³⁷ E.g. Jeffrey Rosen, *The Naked Crowd* 105-06 (Random House 2004).

³⁸ See Remarks, David Jensen, “Data Mining in the Private Sector,” Center for Strategic and International Studies, July 23, 2003; David Jensen, Matthew Rattigan, Hannah Blau, “Information Awareness: A Prospective Technical Assessment,” SIGKDD ’03 (August 2003) (ACM 1-58113-737-0/03/0008).

³⁹ See AP, “Computer-sleuthing aids troops in Iraq,” (Dec. 23, 2003). Any who doubt that, in some form, enhanced information search technology can work need only contemplate the recent arrest of LaShawn Pettus-Brown, whose date identified him as a fugitive when she “Googled” him. See Dan Horn, “Fugitive Done in by Savvy Date and Google,” USA Today (Jan. 29, 2004) (available at http://www.usatoday.com/tech/news/2004-01-29-google-bust_x.htm). Compare that with the pre-September 11 prohibition (eliminated by the new FBI guidelines) on the FBI’s use of Google. See L. Gordon Crovitz, “Info@FBI.gov,” Wall St. J. (June 5, 2002). At some fundamental level the ultimate question is how to reconcile readily available technology in commercial and public use, with the broad governmental monopoly on the authorized use of force. Whatever the proper resolution, we cannot achieve it by hiding our heads in the sand and pretending that data integration technology does not exist.

research question, as yet unanswered, is the actual utility of the system and the precise probabilities of its error rates.⁴⁰

III. Some Speculative Thoughts and Analysis

Innovation – Since my goal here is to do more than address the status quo let me briefly talk about two innovative ideas that have yet to become part of the discussion of CAPPS II generally and that may offer additional technological or programmatic means of improving the system. I offer them here in outline form – they are by no means fully developed.

The first of these is something that K. A. Taipale of the Center for Advanced Studies has called “verified pseudonymity.”⁴¹ In effect, verified pseudonymity, is a form of “traceable anonymity.” It would allow the disclosure of relevant and important information while concealing that which is not necessary to disclose. In the credit card context, for example, a merchant doesn’t need to know the name of the person carrying the card, he only needs to know that the person is entitled to carry the card and that the card can pay the fee. A card with no name, but with a thumbprint, for example, would work. Similarly, in the air transportation context, the traveler might carry a token with a unique, anonymized identifier and that identifier (rather than his name) could be compared to a database of prohibited travelers. The result would produce the answer that TSA wants – whether the person in question is “safe to travel” – without necessarily requiring disclosure of the individuals identity or other attributes. And the virtue of the “traceable” portion of the anonymity is that if a match is made – if, for example, a traveler is identified as a terrorist threat then (and *only* then) could the government (through legal procedures to be determined by Congress) break the anonymity barrier and identify the individual. To be sure, the technology for this sort of solution to the problem is still in its infancy, but I commend it to the Subcommittee’s attention as a possible technological answer to some of the privacy concerns relating to CAPPS II – if only for implementation at a later date.⁴²

The second suggestion is an idea of my own, inspired by some consideration of a “Trusted Traveler” program. Let me return to the paradigm that governs my thinking on CAPPS II – as with the federal judge whose dilemma I described, the problem is not one of a privacy invasion. We have long since passed the point where, for example, one could colorably claim a right to travel anonymously (i.e. pay cash, no identification, no name). So some aspects of a travelers’ privacy will have to be foregone – the question really is which

⁴⁰ One final note – though privacy advocates are concerned about the false positives, the existence of an available system also may create civil tort liability for the failure to deploy. It is not fanciful to imagine tort suits against airlines that either do not implement CAPPS II or refuse to cooperate with TSA if by doing so they give rise to a false negative.

⁴¹ The concept I outline here is discussed in more detail in K. A. Taipale, “Technology, Security, and Privacy: The Legend of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd,” Yale J. Law and Technology (forthcoming) (a discussion draft is available at <http://www.taipale.org/papers/tsp-yjs.htm>).

⁴² Substantially more information on data anonymization mechanisms (as well as privacy permissioning technology and immutable audits) will be available soon in a forthcoming paper being jointly produced by The Heritage Foundation and the Center for Democracy and Technology. See James X. Dempsey & Paul Rosenzweig, “Privacy-Preserving Data Sharing: Technologies That Can Protect Privacy as Information Is Shared for Counterterrorism Purposes” (forthcoming).

aspects an individual is asked to give up. In other words: how much privacy must we give up and in what mixture?

The precise amount of privacy one gives up must, of course, be calibrated to the level of the threat we experience. One could imagine, as a thought experiment, systems in which one were required to give up *all* physical or electronic privacy in order to fly. Thus, we could require all passengers to fly naked, or let nobody fly who had not passed a full Top Secret security background check. Of course, to suggest either course is to recognize how absurd the proposals are.

Or is it? In my view, we should recognize the reality of a privacy trade-off, and also recognize that different people might make different choices. I was struck, for example, by the fact that there already *was* an airline flight known as “Naked Air.” (albeit a bit of a lark).⁴³ Similarly, though the proposed “Trusted Traveler” program will require something equivalent to a security background check for entrants, it has been reported that many business travelers have expressed an interest in the program.⁴⁴ By their choices, Americans are already voicing their preferences.

And that suggests the germ of a further idea – allowing choice for the less frequent traveler of other, more moderate options. We might, for example, envision a system in which a traveler could opt among three possibilities – a “Trusted Traveler” program, a limited electronic screening as embodied in CAPPs II that had on-site electronic screening, and a baggage and personal screening system akin to that which is now randomly applied. Imagine if Americans were empowered to choose – you would be able to either allow an in-depth examination of your personal background (and receive the benefit of no physical screening); a modest examination of your electronic records to verify your identity electronically; or agree to forgo some physical privacy to permit examination of your person and effects. Of course, we would need to know if CAPPs II can work in “real time” at the airport or allow passengers to make the choice at the time they book their trips. Perhaps, given the various values that differing individuals place on different aspects of their privacy, the availability of choice would answer many of the concerns. Again, this is merely a notion, but I offer it for the Subcommittee’s consideration.

Risk Assessment and Resource Allocation – I want to close with one other point that I think is worth your consideration – one that is often not remarked upon. I refer to the distinction between the risk assessment and risk avoidance or reduction. This distinction acknowledges the difference between the analysis aspects of CAPPs II and the screening process itself.

Risk assessment – attempting to determine what risks there are and the likelihood of the threat – is an inexact science. But it is a science -- one that we use in rating risks throughout our experience in the commercial world. It is also, at least in theory, completely distinct from the question of risk avoidance/reduction – that is, how we address the risks

⁴³ Inasmuch as this testimony will be posted to the House web site, I will provide the link for this citation in a modified form to preclude a direct access link. You may view the Naked Air web site at [www “dot” naked-air “dot” com](http://www.dot/naked-air.com).

⁴⁴ Travelocity reports, for example, that 43% of frequent travelers (with more than 5 trips per year) favor the program. See Travel Security Update (Feb. 2002) (available at http://media.corporate-ir.net/media_files/NSD/TVLY/presentations/tvly_022502/sld001.htm).

identified. Risk assessment may inform resource allocation but it does not specify how those resources are employed. In the CAPPS II context, the process of determining which airports are at greater risk is theoretically distinct from the manner proposed for addressing those risks (i.e. screening the individuals who are assessed as more risky).

We could, at least in theory, adopt a system where the CAPPS II screening system did not result in an individual screening determination. Rather, we could use it on a pure resource allocation basis, surging additional TSA screening resources to areas where the threat is perceived and then using those resources to conduct a greater number of random screenings. It could also be used to target at risk flights to allow for the better allocation of limited Federal Air Marshal resources. Even these uses, though less precise than the targeted use envisioned, would be a vast improvement over the current situation. Today, for example, TSA screeners are distributed throughout the system based not upon an assessment of risk but rather on the volume of traffic at an airport. Implicit in this assignment is either the assumption that risk is directly proportional to the volume of traffic or a conscious decision to disregard risk assessment – the former is a gross over-generalization and the latter is simply unwise and ineffective.

CAPPS II promises a change – we can envision the day when TSA inspectors (and other resources such as Air Marshals), are allocated in the way we think best addresses actual risks of harm, increasing the chances of catching terrorists and minimizing the unnecessary intrusion into people's lives at times and places where there is no risk at all. Should Congress have any concerns at all about the intrusiveness of individual screening it should, at a minimum, recognize the utility of enhanced risk assessment technology. To fail to do so would be even worse than our current system.

* * * * *

In short, CAPPS II has some significant issues that need to be addressed. But it also is a system of great promise. Failing to make the effort to use new technology wisely poses grave risks and is an irresponsible abdication of responsibility.

As six former top-ranking professionals in America's security services recently observed, we face two problems—both a need for better analysis and, more critically, “improved espionage, to provide the essential missing intelligence.” In their view, while there was “certainly a lack of dot-connecting before September 11,” the more critical failure was that “[t]here were too few useful dots.”⁴⁵ CAPPS II technology can help to answer both of these needs. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11 pointed out in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between

⁴⁵ Robert Bryant, John Hamre, John Lawn, John MacGaffin, Howard Shapiro & Jeffrey Smith, “America Needs More Spies,” *The Economist*, July 12, 2003, p. 30.

Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively . . .*⁴⁶

Or, as one commentator has noted, the reflexive opposition to speculative research by some is “downright un-American.”⁴⁷ Though CAPPs II technology might prove unavailing, the only certainty at this point is that no one knows. It would be particularly unfortunate if Congress opposed basic scientific research without recognizing that in doing so it was demonstrating a “lack [of] the essential American willingness to take risks, to propose outlandish ideas and, on occasion, to fail.”⁴⁸ That flaw is the way to stifle bold and creative ideas—a “play it safe” mindset that, in the end, is a disservice to American interests.

Mr. Chairman, thank you for the opportunity to testify before the Subcommittee. I look forward to answering any questions you might have.

⁴⁶ *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi (available at http://www.fas.org/irp/congress/2002_rpt/911rept.pdf) (emphasis supplied). The Joint Inquiry also critiqued the lack of adequate analytical tools, *id.* Finding 5, and the lack of a single means of coordinating disparate counterterrorism databases, *id.* Findings 9 & 10. Again, aspects of the CAPPs II program are intended to address these inadequacies and limitations on the research program are inconsistent with the Joint Inquiry’s findings.

⁴⁷ See David Ignatius, “Back in the Safe Zone,” *The Washington Post*, August 1, 2003, p. A19.

⁴⁸ *Id.*

Statement of
David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the
House Committee on Transportation and Infrastructure
Aviation Subcommittee

**“The Status of the Computer-Assisted Passenger
Prescreening System (CAPPS II)”**

March 17, 2004

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to address the privacy and civil liberties implications of the enhanced Computer Assisted Passenger Prescreening System (“CAPPS II”) now under development within the Transportation Security Administration (“TSA”). The subcommittee’s inquiry is critically important and goes to one of the most significant controversies surrounding the government’s response to the tragic events of September 11, 2001. While most of the post-9/11 debate over security and liberty understandably has focused on the USA PATRIOT Act, the serious problems inherent in CAPPS II will have a more direct and immediate impact on most Americans. The CAPPS II mission – to conduct background checks on tens of millions of citizens – is unprecedented in our history. While we all agree that there is a clear need for enhanced aviation security, there are many reasons to question whether CAPPS II is the right approach, both from a security perspective and in terms of its detrimental impact on our traditional liberties.

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the “‘constitutional right to travel from one State to another’ is firmly embedded in our jurisprudence.”¹ For that reason, any governmental initiative, such as CAPPS II, that conditions the ability to travel upon the surrender of privacy

¹ 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

and due process rights requires particular scrutiny. I hope that today's hearing marks the beginning of a serious inquiry into the costs and claimed benefits of CAPPs II, and that there can be an informed public debate on the proposal – a debate that has not yet occurred. Critical elements of that discussion, which I will address today, include transparency, due process and adherence to established privacy principles.

The problems that are likely to arise if and when CAPPs II becomes operational are not hypothetical. For more than two years, an untold number of innocent airline passengers have been wrongly flagged as a result of TSA's secretive "selectee" and "no-fly" lists. Documents obtained by EPIC under the Freedom of Information Act detail the Kafkaesque dilemmas that scores of citizens have confronted when they attempt to learn why they are consistently flagged and seek to clear their names.² TSA refuses to provide these individuals with any explanations, and the agency's claimed procedure for addressing these problems, as USA Today noted, "is cumbersome, confusing and – the TSA concedes – doesn't guarantee success."³

Although few details of CAPPs II have been disclosed, the Privacy Act notice for the system that TSA published on August 1, 2003,⁴ provides a basic outline of how it would operate. In essence, CAPPs II will be a secret, classified system that the agency will use to conduct background checks on tens of millions of airline passengers. The resulting "risk assessments" will determine whether individuals will be subject to invasive searches of their persons and belongings, or be permitted to board commercial aircraft at all. TSA will not inform the public of the categories of information contained in the system. It will include information that is not "relevant and necessary" to accomplish its stated purpose of improving aviation security. Individuals will have no judicially enforceable right to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. It is important to note that this is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.⁵

² See http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html

³ *Glitches Repeatedly Delay Innocent Air Travelers*, USA Today, June 25, 2003, Page 11A.

⁴ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

⁵ 5 U.S.C. § 552a.

Given its constitutional implications, and the massive scope of the system (which seeks to collect information about tens of millions of individuals), CAPPS II understandably has been the focus of concern within Congress and the general public. It has also engendered strong opposition abroad, where foreign governments and their citizens have resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States. Reflecting those concerns, a resolution was passed last September at the International Conference of Data Protection and Privacy Commissioners in Sydney, Australia calling for “an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to data subjects, the assurance of data subject rights and independent supervision” before such data transfers occur.⁶

Much of the controversy surrounding CAPPS II has centered on the system’s secrecy and the lack of public information concerning the manner in which it will assess the security risks particular individuals are deemed to pose, and the types of data that TSA will use to make such assessments. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.⁷ The Privacy Act is intended “to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]”⁸ Adherence to these requirements is critical for a system like CAPPS II.

In remarks before the international conference of data protection and privacy officials, the Chief Privacy Officer of the Department of Homeland Security assured the delegates that

[u]nder the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government’s activities and the federal government’s use of personal information about them.⁹

⁶ Resolution Concerning the Transfer of Passengers’ Data, 25th International Conference of Data Protection & Privacy Commissioners (September 12, 2003) (available at <http://www.epic.org/news/Comm03.html>).

⁷ S. Rep. No. 93-1183, at 1 (1974).

⁸ *Id.*

⁹ Remarks of Nuala O’Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney Australia, September 11, 2003 (“Kelly Remarks”).

Unfortunately, the Department of Homeland Security and TSA have fallen far short of such transparency in the realm of aviation security.

The Lack of Transparency Surrounding CAPPS II

Soon after enactment of the Aviation and Transportation Security Act, Pub. L. No. 107-71, and the creation of TSA, EPIC began requesting information from the agency under the Freedom of Information Act seeking information on the potential privacy impact of CAPPS II. TSA has strenuously resisted the disclosure of virtually all relevant information, so there is only a sparse public record concerning the system's proposed operation.

One of EPIC's FOIA requests sought the release of TSA's Privacy Impact Assessment ("PIA") and the "Capital Asset Plan and Business Case" for the CAPPS II project. On September 25, 2003, TSA responded to the request and advised EPIC that both documents exist only in draft form and that "final versions . . . are not expected until early 2004."¹⁰ To date, these documents have not been made public. The fact that the PIA and Business Case have not been finalized is significant because their preparation for a system such as CAPPS II is mandated by the E-Government Act and Office of Management and Budget ("OMB") regulations, respectively. The E-Government Act requires that agencies "*shall* conduct a privacy impact assessment . . . *before* . . . initiating a new collection of information that . . . will be collected, maintained, or disseminated using information technology."¹¹ Likewise, OMB regulations require agencies, when proposing "major" or "significant" information technology projects, to address privacy and security issues in their Business Case submissions and to prepare PIAs.¹²

In his testimony before Congress on May 6, 2003, then-TSA Administrator Loy stated that "TSA is mindful that privacy protections must be built into the CAPPS II system from its very foundation" and said that the agency was "working to finalize its CAPPS II business case, which will detail how privacy and security are built into the system" and "also will conduct a

¹⁰ Letter from Patricia M. Riep-Dice to David L. Sobel, September 25, 2003 (available at <http://www.epic.org/privacy/airtravel/pia-foia-response.pdf>).

¹¹ Pub. L. No. 107-347 (December 17, 2002), § 208 (emphasis added).

¹² OMB Circular A-11, part 3, Planning, Budgeting and Acquisition of Capital Assets (July 2000); Memorandum from Joshua B. Bolton, "Implementation Guidance for the E-Government Act of 2002" (August 1, 2003) (available at <http://www.whitehouse.gov/omb/memoranda/m03-18.pdf>).

Privacy Impact Assessment.”¹³ It is thus surprising to find TSA continuing to move ahead with CAPPS II before the privacy implications of the system have been fully addressed and disclosed to the public. Indeed, the recent General Accounting Office (“GAO”) report on CAPPS II underscores that fact. The GAO, in a report on another DHS information system, noted that “OMB requires that IT projects . . . perform a system privacy impact assessment, so that relevant privacy issues and needs are understood and appropriately addressed *early and continuously* in the system life cycle.”¹⁴ CAPPS II has been under development for more than two years; it is clear that TSA has failed to meet its obligation to address the privacy implications “early and continuously,” as federal law requires. We cannot have an informed public debate on the implications of CAPPS II unless and until TSA publishes a Privacy Impact Assessment and discloses other information about the system. Unfortunately, as I will explain in my discussion of the CAPPS II Privacy Act notice issued by TSA, lack of transparency is likely to be a key characteristic of the system.

CAPPS II Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens’ privacy interests against government intrusion. Congress found that “the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies,” and recognized that “the right to privacy is a personal and fundamental right protected by the Constitution of the United States.”¹⁵ It thus sought to “provide certain protections for an individual against an invasion of personal privacy” by establishing a set of procedural and substantive rights.¹⁶

DHS’s Chief Privacy Officer recently touted the protections afforded by the Privacy Act, explaining that the law

¹³ Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003) (“May 6 Loy Testimony”).

¹⁴ INFORMATION TECHNOLOGY: Homeland Security Needs to Improve Entry Exit System Expenditure Planning, GAO-03-563 (June 2003) (emphasis added).

¹⁵ Pub. L. No. 93-579 (1974).

¹⁶ *Id.*

provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed “system of records” notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one’s own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.¹⁷

TSA, however, has sought to exempt CAPPS II from nearly all of the Privacy Act provisions Ms. O’Connor Kelly described.¹⁸

1. TSA Will Not Disclose the Sources of Information Fed Into CAPPS II

Under the Privacy Act, government transparency is the rule rather than the exception. TSA has frustrated that intent by exempting the CAPPS II system of records from the requirement that it publish “the categories of sources of records in the system.”¹⁹

The legislative history of the Privacy Act unequivocally demonstrates that government agencies must be open about their information collection practices unless they can show that exceptional circumstances require secrecy. One key objective of the Privacy Act is to ensure that agencies “give detailed notice of the nature . . . of their personal data banks and information systems”²⁰ The Senate Report notes that “it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency.”²¹ In those few instances in which a limited exemption for national security and law enforcement was recognized, the exemption was “not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information.”²² Rather, the agency must show that the

¹⁷ Kelly Remarks.

¹⁸ Indeed, TSA has invoked exemptions for *all* of the requirements that the Privacy Act permits an agency to invoke.

¹⁹ 5 U.S.C. § 552a(e)(4)(I); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

²⁰ S. Rep. No. 93-1183, at 2 (1974).

²¹ *Id.* at 74.

²² *Id.*

implementation of specific Privacy Act provisions would “damage or impede the purpose for which the information is maintained.”²³

In its authoritative guidance on implementation of the Privacy Act, OMB explained that “[f]or systems of records which contain information from sources other than the individual to whom the records pertain, the notice should list the types of sources used.”²⁴ While “[s]pecific individuals or institutions need not be identified,” the Act contemplates that general categories, such as “financial institutions” or “educational institutions” should be listed.²⁵

Despite the Privacy Act’s clear emphasis on transparency and TSA’s claimed dedication to preserving individuals’ privacy, the agency seeks to avoid the requirement that it inform the public of the sources of information that will feed into the CAPPS II system. TSA has not even attempted to meet its burden of demonstrating that the publication of such basic information about the system would somehow impede its presumed effectiveness.

In the supplementary material accompanying its Privacy Act notice, TSA asserted that it “will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination.”²⁶ That assurance rings hollow, however, in light of the agency’s stated intention to keep secret the sources of information that will eventually be fed into the system.

TSA’s determination that CAPPS II will be exempt from the requirement of publishing categories of sources of records is at odds with specific assurances the agency provided to Congress. When asked about this issue last May, Admiral Loy indicated that such information would, in fact, be disclosed:

Senator Byrd: Will the new notice name the precise databases of information that CAPPS II will collect about air passengers?

Admiral Loy: I don’t know that we have any reason not to name those in the privacy notice²⁷

²³ *Id.* at 75.

²⁴ OMB Guidelines at 28964.

²⁵ *Id.*

²⁶ Interim Final Privacy Act Notice, 68 Fed. Reg. 45263, 45267.

²⁷ *The Fiscal Year 2004 Appropriations for the Bureau of Customs and Border Security; Transportation Security Administration and Federal Law Enforcement Training Center, Hearing Before the Homeland Security*

If TSA cannot articulate any reason to exempt CAPPS II from publishing categories of sources of records, it should not exempt the system from that requirement. The Privacy Act does not permit such secrecy unless an agency can demonstrate that it is absolutely necessary for reasons of national security and law enforcement.

2. TSA Will Not Provide Meaningful Citizen Access to Personal Information

In its Privacy Act notice, TSA has exempted CAPPS II from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;²⁸ and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.²⁹

In lieu of the statutory, judicially enforceable right of access provided by the Privacy Act, TSA plans to establish the “CAPPS II Passenger Advocate,” apparently to act as a sort of ombudsman, to receive and process requests for access. According to the supplementary information accompanying TSA’s notice, “passengers can request a copy of *most* information contained about them in the system from the CAPPS II passenger advocate.”³⁰ The formal notice section, however, states that “[a]ll persons may request access to records containing information *they* provided,” which presumably would include only the name, address, and telephone number given to an airline when making a travel reservation.³¹ In addition, the notice provides that the system of records “may not be accessed for purposes of determining if the

Subcommittee of the Senate Appropriations Committee, 108th Cong. (May 13, 2003) (testimony of Admiral James Loy).

²⁸ 5 U.S.C. § 552a(d)(1). Individuals may seek judicial review to enforce the statutory right of access provided by the Act. 5 U.S.C. § 552a(g)(1).

²⁹ 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).

³⁰ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267 (emphasis added).

³¹ *Id.* at 45269 (emphasis added).

system contains a record pertaining to a particular individual.”³² Such limited, discretionary access to information is an inadequate substitute for the access provisions set forth in the Privacy Act, and TSA offers no explanation why such restricted access is necessary in the context of CAPPS II.

TSA’s “passenger advocate” acting as middleman is no substitute for the judicially-enforceable access rights provided by the Privacy Act. TSA’s notice states that access to one’s personal information may be obtained “by sending a written request to the CAPPS II Passenger Advocate” and that “to the greatest extent possible and consistent with national security requirements, such access will be granted.”³³ No time guidelines are specified for the procedure. However, TSA explains that “in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system” because records are maintained for too short a time, although “[t]he duration of data retention” for non-U.S. persons “is still under consideration,” and “[e]xisting records obtained from other government agencies, including intelligence information, watch lists, and other data will be retained for three years, or until superseded.”³⁴

As a practical matter, therefore, the only information a passenger would be able to access is the information he provided to the airlines himself. Moreover, even this information may not be accessible, as that information will likely be destroyed in the time it takes a passenger to contact the passenger advocate. In most cases, a passenger will be unable to gain access to records about him kept by the agency, and, in many cases, he will not even be able to learn that a record pertaining to him exists. In fact, the only indication a passenger may have that the government is keeping records about him is if he is subjected to extra scrutiny at the security gate (or, of course, detained and arrested there). TSA’s weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies.

³² *Id.*

³³ *Id.*

³⁴ *Id.*

3. TSA Will Not Provide Citizens Meaningful Opportunities to Correct Inaccurate, Irrelevant, Untimely and Incomplete Information

Companion and complementary to the right to access information is the right to ensure that it is accurate. TSA's Privacy Act notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted the CAPPS II system from the Privacy Act requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;³⁵
- an agency must make notes of requested amendments within the records;³⁶ and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.³⁷

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.³⁸

Instead of the judicially enforceable right to correction set forth in the Privacy Act,³⁹ TSA has established its own, discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notice states that "[a] passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request

³⁵ 5 U.S.C. § 552a(d)(2)(B), (d)(3).

³⁶ 5 U.S.C. § 552a(d)(4).

³⁷ 5 U.S.C. § 552a(f)(4).

³⁸ H.R. Rep. No. 93-1416, at 15 (1974).

³⁹ 5 U.S.C. § 552a(g)(1).

to the CAPPS II Passenger Advocate.”⁴⁰ Further, “[i]f the matter cannot be resolved by the CAPPS II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office.”⁴¹ Notably, TSA reserves the right to alter even these minimal, discretionary procedures: “These remedies for all persons will [be] more fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational.”⁴² In addition, “DHS is currently developing a robust review and appeals process, to include the DHS privacy office.”⁴³

The notice provides TSA the discretion to correct erroneous information upon a passenger’s request, but does not obligate the agency to do so. Significantly, there would be no right to judicial review of TSA’s determinations. This correction process offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at TSA’s whim. Furthermore, the agency presents no explanation why judicially-enforceable Privacy Act correction procedures would be inappropriate in the context of CAPPS II. Denying citizens the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that CAPPS II will be an error-prone, ineffective means of singling out passengers as they seek to exercise their constitutional right to travel.

4. CAPPS II Will Not Be Limited to Collection of Information That Is “Relevant and Necessary”

Incredibly, TSA has exempted CAPPS II from the fundamental Privacy Act requirement that an agency “maintain in its records only such information about an individual as is relevant and necessary” to achieve a stated purpose required by Congress or the President.⁴⁴ TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the CAPPS II system that is irrelevant and unnecessary, although it apparently intends to do so. Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act

⁴⁰ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ 5 U.S.C. § 552a(e)(1); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

and raises serious questions concerning the likely impact of the CAPPS II rating process on millions of law-abiding travelers.

In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The “relevant and necessary” provision

reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government’s needs, its actions may not be arbitrary[.]⁴⁵

As OMB noted in its Privacy Act guidelines, “[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful.”⁴⁶

The Privacy Act’s “relevant and necessary” provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government’s stated (and legally authorized) objective. Like TSA’s other deviations from customary Privacy Act requirements, the “relevant and necessary” exemption will serve only to increase the likelihood that CAPPS II will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing aviation security.

5. Broad “Routine Uses” of CAPPS II Data Will Exacerbate the System’s Privacy Problems

TSA’s Privacy Act notice identifies six categories of “routine uses” of the information that will be collected and maintained in the CAPPS II system of records.⁴⁷ These include anticipated disclosure to a broad range of individuals and entities, such as “Federal, State, local,

⁴⁵ S. Rep. No. 93-3418, at 47 (1974).

⁴⁶ OMB Guidelines at 28960.

⁴⁷ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

international, or foreign agencies or authorities . . . contractors, grantees, experts, or consultants . . . airports and aircraft operators.”⁴⁸ As noted, the information that would be disclosed is likely to include material about individuals that is not “relevant and necessary” to any legitimate aviation security requirements. Nor would such information be subject to a meaningful and enforceable process to ensure that it is accurate, relevant, timely or complete. The broad dissemination of CAPPS II information that TSA anticipates underscores the need for full transparency (and resulting public oversight) and judicially-enforceable rights of access and correction.

Related to the breadth of the routine uses is the issue of “mission creep” – the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. Admiral Loy discussed the issue in Congressional testimony, stating that “mission creep, if you will, is one of those absolute parameters that . . . I am enormously concerned about and we will build such concerns into the privacy strategy that we will have for CAPPS II.”⁴⁹ Three months before the notice was published, Admiral Loy assured Congress that CAPPS II was designed as an aviation security tool, and not as a law enforcement tool.⁵⁰

Despite those assurances, the CAPPS II system already contains a carve-out for a purpose beyond its original mission. The Privacy Act notice states that “[a]fter the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence may also be analyzed in the context of this system.”⁵¹ While the government clearly has a legitimate interest in apprehending accused felons, there are innumerable reasons why it may want to locate particular individuals. Such uses of CAPPS II data, however, are plainly beyond the authorized scope of TSA’s mission of

⁴⁸ *Id.*

⁴⁹ May 6 Loy Testimony.

⁵⁰ *Id.* Admiral Loy stated:

[w]e are not searching [the National Crime Information Center database] as part of the . . . data that we’re looking at . . . [A]t the moment we are charged with finding in the aviation sector foreign terrorists or those associated with foreign terrorists and keep[ing] them off airplanes. That is our very limited goal at the moment. . . . [E]ven as heinous as it sounds, the axe murderer that gets on the airplane with a clean record in New Orleans and goes to Los Angeles and commits his or her crime, that is not the person we are trying to keep off that airplane at the moment.

⁵¹ Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45266.

ensuring aviation security. It is crucial that TSA define the purpose of CAPPS II, at the outset, more strictly and limit the use of collected information to its core mission.

Testing of CAPPS II Should Not Proceed Until TSA's Notice is Revised

While TSA has stated that “[a] further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system,”⁵² it also indicated in its August notice that “[w]ith the publication of this notice, internal systems testing will begin, using this System of Records.”⁵³ According to the agency, “[d]uring these tests, TSA will use and retain [Passenger Name Record] data for the duration of the test period.”⁵⁴ It has been reported that TSA is contemplating the issuance of a security directive requiring U.S. airlines to provide the agency with passenger information for use in the testing process.⁵⁵ Such data acquisition would place in the agency's hands personal information concerning millions of individuals without, as I have discussed, meaningful rights of access or correction. TSA has articulated no reason why such rights should not be provided and, as such, even limited use of personal information for testing purposes would raise significant privacy issues. Acquisition of personal data should not proceed until TSA revises its policies and practices to bring them into conformance with the intent of the Privacy Act.

⁵² *Id.*

⁵³ *Id.* at 45265-45266.

⁵⁴ *Id.* at 45267.

⁵⁵ Sara Kehaulani Goo, *TSA May Try to Force Airlines to Share Data*, Washington Post, September 27, 2003, Page A11. It is unclear whether TSA plans to compel passenger data from airlines through a security directive or a proposed rulemaking. The GAO report on CAPPS II states:

TSA officials stated that they are continuing to seek needed passenger data for testing, but believe they will continue to have difficulty in obtaining data for both stress and other testing until TSA issues a Notice of Proposed Rulemaking to require airlines to provide passenger data to TSA. This action is currently under consideration within TSA and DHS.

AVIATION SECURITY: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385 (February 2004).

Conclusion

As the recent GAO report found, TSA has failed to adequately address the very real privacy and due process issues that permeate the proposed system. Based upon TSA's Privacy Act notice for the system, I believe there is reason to doubt whether the system, as currently envisioned, can ever function in a manner that protects privacy and provides citizens with basic rights of access and redress. In order for CAPPS II to pass muster from a privacy and civil liberties perspective, TSA must, at a minimum: 1) ensure greater transparency through the establishment of a non-classified system; 2) provide individuals enforceable rights of access and correction; 3) limit the collection of information to only that which is necessary and relevant; and 4) substantially limit the routine uses of collected information. Further, development of the system should be suspended until TSA prepares a final Privacy Impact Assessment, discloses it to the public and receives public comments. Finally, the agency should not acquire personal information, even for testing purposes, until it has revised its policies and procedures as suggested above.

Thank you for the opportunity to address the serious privacy and due process implications of CAPPS II, and for your consideration of the critical issues raised by the proposed system. I encourage the subcommittee to continue its inquiry and to ensure that the privacy and due process rights of airline passengers are preserved as we develop effective and appropriate aviation security measures.

DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

STATEMENT OF

DAVID M. STONE
ACTING ADMINISTRATOR

ON
THE SECOND GENERATION COMPUTER ASSISTED PASSENGER
PRESCREENING SYSTEM
(CAPPS II)

BEFORE THE
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON AVIATION
UNITED STATES HOUSE OF REPRESENTATIVES

March 17, 2004

Good morning Mr. Chairman, Congressman DeFazio, and Members of the Subcommittee. I am pleased to have this opportunity to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss the status of the Second Generation of the Computer Assisted Passenger Pre-Screening System (CAPPS II). The Department of Homeland Security (DHS) and TSA firmly believe that development of CAPPS II is a vital ring in our system of systems approach to aviation security and we are working to quickly resolve remaining policy and privacy concerns in order to proceed with testing. The description in this testimony is the current vision of how CAPPS II will work.

As part of the Aviation and Transportation Security Act (ATSA) (P.L. 107-71), Congress directed that the Secretary of Transportation ensure that "the Computer-Assisted Passenger Prescreening System, or any successor system – is used to evaluate all passengers before they board an aircraft; and includes procedures to ensure that individuals selected by the system and their carry-on and checked baggage are adequately screened."¹ This requirement became part of the mission of TSA, with overall responsibility transferring with TSA to DHS on March 1, 2003, as provided for in the Homeland Security Act of 2002.

Before discussing CAPPS II, and the vital impact it will have on aviation security, it is important to discuss the limitations of the current first generation passenger prescreening system – CAPPS. This system was jointly developed in the mid 1990s. It is operated by the airlines, not the Federal Government, and according to the industry, costs approximately \$150 million per year to operate. CAPPS does not use a centralized

¹ ATSA, §136, amending 49 U.S.C. §44903.

structure; rather, each air carrier determines how best it can prescreen passengers under CAPPS. In some cases air carriers are able to electronically prescreen the passengers through their information technology system. In other cases, however, an air carrier must use paper lists of passengers who must be flagged for further security screening. This is too costly, time consuming, and error prone a method of prescreening passengers, especially in the wake of the 9/11 attacks on this country.

The rules CAPPS uses to select passengers for enhanced screening do not reflect today's threats to aviation. They flag large numbers of airline passengers because of innocent ticket purchase habits. These passengers then require enhanced screening, even though they may pose no discernible threat to aviation security. This is frustrating to passengers, and forces TSA to allocate resources to conduct extensive screening of a population that does not require it.

I am sure that the Members of this Subcommittee know full well that air carrier passengers complain that travelers who do not appear to pose a threat to aviation security are nevertheless selected for enhanced screening. TSA is also fully aware of these complaints. We also hear complaints from passengers who are incorrectly identified as being on government watch lists and recognize that these people must go through a time consuming and frustrating process to differentiate themselves from those individuals who are properly on the lists.

The reality of the situation, however, is that every day about 1.8 million passengers present themselves at airport security checkpoints and must be screened, yet the current CAPPS program provides little information on who these 1.8 million passengers are or whether they pose any threat to aviation security. As a result, TSA must perform additional screening to provide the level of security that we and the American public demand. That is in large part why we are developing CAPPS II, which includes a critical identity authentication component.

Because the first generation of CAPPS does not do enough to enhance aviation security, and because Congress directed, in ATSA, that any successor system must evaluate all passengers before they board an aircraft, TSA is working diligently to develop CAPPS II. This second generation prescreening system will be a centralized, automated, threat-based, real time, risk assessment platform. It will increase our ability to ensure the people are designated for secondary screening by using best practice identity authentication procedures combined with a risk assessment. A final aspect of prescreening being considered for CAPPS II, which I will discuss later, involves detecting individuals who are the subject of an outstanding Federal or state warrants for violent crimes.

CAPPS II is being designed to take the burden of operating the current CAPPS system from the airlines and will centralize all commercial verification and government data sharing and analyses under government control. This will allow CAPPS II to move beyond the current rules based system that uses only limited passenger itinerary information to determine screening level. CAPPS II is expected to employ technology

and data analysis techniques to conduct an information-based, identity authentication for each passenger using commercial information along with data each passenger provides to the airline upon making a reservation, along with information resident in airline reservation systems. CAPPS II will combine the results (scores) from the identity authentication with a risk assessment. Unlike the existing CAPPS system, CAPPS II will have built-in auditing capabilities and privacy protections, and will include a redress mechanism for passengers who believe that they have been incorrectly selected for additional screening or, in rare cases, misidentified as a threat. As currently designed, the entire process of vetting a passenger through CAPPS II should take a short amount time to accomplish, measured in seconds.

Currently, the CAPPS II system is being designed to perform the following functions:

- Obtain available Passenger Name Record (PNR) data from airlines and computer reservation systems. At a minimum this data will include full name, home address, home telephone number, and date of birth;
- Authenticate each passenger's identity using commercial companies providing authentication services. Specifically, commercial data aggregators will perform an identity authentication for each passenger using techniques traditionally applied to validate identity. The data aggregators will provide to CAPPS II a score reflecting the degree of certainty that the passengers are who they say they are. These commercial data aggregators will be prohibited by contract from using the PNR data obtained through the CAPPS II process for any other purpose, including commercial or marketing uses and they will not transmit to the government any of the public source information they will use to authenticate a passenger's identity. Compliance will be audited and enforced in real time by a National Security Agency (NSA) certified data guard that will permit monitoring use of such data and enable actions to be taken in response to any infringements;
- Compare the passenger identity information against the Terrorist Screening Center's consolidated terrorist screening database, and against lists of individuals who are the subject of outstanding warrants for violent criminal behavior maintained by U.S. Government data sources;
- Assess other risks based on current terrorist-related threat information;
- Disseminate the threat results to the appropriate airport screening or airport law enforcement authorities with sufficient advance notice (approximately 72 hours before flight takeoff, and again in the event of a last-minute ticket purchase or any passenger-initiated change in itinerary) in order to allocate necessary response resources. Initially, results will be sent to the airline reservation systems for encoding on the passenger's boarding pass; and
- Distribute to screening staff through code on boarding passes the necessary screening level for each passenger.

The possible categories of screening are as follows²:

- *Low risk*: passenger boards after routine screening;
- *Elevated or unknown risk*: the passenger will be subject to additional security screening prior to boarding (in overseas locations, TSA will need to work with appropriate officials in the host country to ensure additional security screening is conducted in accordance with that country's laws and screening procedures); and
- *Specific identifiable terrorist threat*: TSA will alert appropriate law enforcement authorities.

As stated earlier, our current modeling suggests that CAPPS II will result in substantially fewer passengers falling into the category of "elevated or unknown risk." Furthermore, we expect that annually no more than a handful of passengers will fall into the category of a "specific identifiable terrorist threat" that will require TSA to notify Federal, state, or local law enforcement agencies. Again, this number is far fewer than those that are brought to the attention of law enforcement agencies under the current airline operated prescreening system.

Unfortunately, there is a tremendous amount of misunderstanding regarding the development of CAPPS II. Certainly, in a democratic society, we should engage in a healthy debate about an individual's right to privacy and the right of the polity to protect itself and its citizens from acts of terrorism. But in order for this debate to be joined, it is necessary to fully understand the facts.

CAPPS II will not be an intelligence gathering system. CAPPS II will not be a data mining system. CAPPS II will not discriminate against individuals because of their race, religion, ethnicity, physical appearance, or economic strata. Individuals who have issues of credit worthiness will not be flagged for enhanced screening, or denied boarding. The key issues for prescreening are simply identity authentication – making sure passengers are who they say they are – augmented by intelligence information that can help us focus screening efforts.

We are designing CAPPS II so it will not maintain data files on passengers beyond the time necessary to complete their itineraries. CAPPS II will not access or contain records of credit card purchases made by passengers (although a passenger's credit card number may appear in airline booking information transmitted to the system) nor will it access or obtain information concerning what medicines passengers may buy, where they shop, or their lifestyles. The only information passed through the CAPPS II firewall from commercial data aggregators will be a generic score indicating confidence in the passenger's identity. This information is far less detailed than the information these same data aggregators provide in the commercial marketplace.

² Some passengers may also be selected for additional security screening based on random selection.

The privacy rights of individuals will be fully respected. TSA is working closely with the DHS Privacy Officer to ensure that this occurs. We have issued two Interim Privacy Act notices to date.³ DHS has committed to issuing a Final Notice before the system becomes operational. This Final Notice will further refine the parameters on the use and retention of passenger data. As required by the E-Government Act of 2002 (P.L. 107-347), we will conduct and publish a Privacy Impact Assessment before the system becomes operational. We will also provide adequate notice to future passengers as required by the Privacy Act. This process will explain to passengers how their information is being used (subject to the requirements of national security) and what rights they have to complain or to seek a remedy. Current plans call for layered notices, beginning with publication in the Federal Register and on the DHS/TSA Web site. Because passenger information will be collected at the point of reservation, TSA will also work with the airlines and reservation agents to generate ideas for providing and documenting this important notice.

We will fully implement safeguards and protocols to ensure that no data gathered as part of a CAPPS II assessment will be made available for any commercial purposes, nor breached by computer hackers, nor subject to improper use by either Government or contractor employees. I would like to describe in detail some of these measures we are planning to take.

The CAPPS II system itself will be secure, and it will only be accessible to persons who require access for the performance of their duties as Federal employees or contractors to the Federal government. The guiding principle for access will be "need-to-know." Access will be compartmentalized, thus allowing access to persons based only on their individual need-to-know and only to the extent of their authorization (*e.g.*, a person might be permitted to access information with regard to the unclassified portion of the system, but be denied access to classified areas). A 24-hour audit trail will be used to monitor all persons accessing or attempting to access the system and will help to ensure compliance with access rules. Because the CAPPS II system will be entirely electronic, the audit trail will immediately and accurately document which individuals have had access to what information in the system.

TSA will take a multi-dimensional approach to safeguarding passenger data. The information is proactively protected in the network, the system, the application, and the monitoring of the system. Key components will be certified by the National Information Assurance Partnership to ensure that they adhere to a security rubric defined by the U.S.-sponsored, international Common Criteria for Information Technology Security Evaluation. Additionally, at the site where CAPPS II processing occurs, numerous operational, physical, and technical controls will ensure that only authorized individuals or systems may connect to the CAPPS II infrastructure. Each piece of the architecture operates in concert with the others to create a robust information assurance program.

We expect the data communications network to be a fundamental building block for the exchange of data between airlines and the CAPPS II system. Therefore, it is critical to

³ January 15, 2003 and August 1, 2003.

note that the infrastructure will be a private, dedicated network. Thus, it will not be directly accessible via public networks, such as the Internet. Moreover, the network will employ multiple information assurance features to ensure the confidentiality, integrity, and availability of data exchange. Data exchange will be protected end-to-end through encryption between the CAPPS II system and the intended, designated airline or security screening end-point. Encryption will ensure that data cannot be reviewed, modified, or removed while in transit. Additionally, as data is received by the CAPPS II infrastructure, it will pass through a multi-tiered firewall to prevent unauthorized access to the system.

The systems upon which the CAPPS II applications will run form another of the security building blocks. During the commissioning of each system, a thorough information assurance evaluation will be undertaken. As part of this activity, systems will be “hardened,” addressing known vulnerabilities and establishing a rigorous security posture. Each of the systems will be protected through the use of specialized security software designed to identify and respond to unexpected or unauthorized changes in the operating environment. Regular review of system audit records will ensure that potential problems are addressed and corrected expeditiously. Finally, proactive testing of the systems, so called “white-hat hacking,” will keep the CAPPS II system’s security posture constantly under internal review.

We will ensure that the applications that form the CAPPS II system safeguard information through arbitration of access control. This arbitration is based primarily on the application’s ability to authenticate entities and processes. Every interaction within the CAPPS II system, from the receipt of data through processing and response, will require the subcomponents of the system to authenticate with one another. Additionally, in the case of remote entities, such as airlines, the system will be able to authenticate using digital certificates, a widely-used, robust form of verification. By using digital certificates, the CAPPS II applications will be able to interact with trusted, known entities. Additionally, data may be encrypted within the CAPPS II system to prevent the unauthorized release of any PNR data.

The final safeguarding component, the monitoring system, will view CAPPS II in a more holistic manner. Correlating information from the network, the systems, and the applications, the monitoring system will constantly generate a picture of the overall security posture of the system. Augmented by the use of Intrusion Detection sensors on the network and in the systems, the monitoring system will form a risk management platform that alerts CAPPS II staff to anomalous or troublesome events across the system. The clear benefit of this component is an ability to quickly identify a series of seemingly unrelated events which taken separately are no cause for alarm, but taken on the whole, warrant an investigation and corrective action.

In response to privacy concerns, CAPPS II will only retain passenger information for U.S. persons for a short period after the completion of a passenger’s flight itinerary – currently estimated at between 72 hours and one week. After that period has passed,

there will be no information that CAPPS II can easily access in a useable format related to individual passengers, should there be a desire to do so.

We are designing a redress process that will allow passengers to submit complaints to TSA regarding CAPPS II. An essential part of the redress process is the establishment of the CAPPS II Passenger Advocate. The Passenger Advocate will focus on assisting passengers who feel that they have been incorrectly or consistently prescreened. When a passenger submits a complaint, and provides the Government with permission to observe and monitor the results of prescreening during the complainant's future flights, TSA will work with other government agencies and commercial data providers to analyze the results of prescreening. This analysis will determine if the complaint is related to prescreening or due to another part of the screening process (e.g., random selection) and determine if selection by CAPPS II is related to data that may be appropriately corrected. Passengers will be afforded the opportunity to appeal these results to TSA HQ and then, in turn, to the DHS Privacy Office.

An important benefit of CAPPS II's identification authentication function can provide is to reduce greatly the number of passengers who are incorrectly identified as being on a U.S. Government terrorist watch-list. In addition, CAPPS II will use the consolidated terrorist screening database that TSC is currently implementing. Under the terms of the Memorandum of Understanding establishing the TSC, signed by the Secretary of State, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, the TSC is also developing quality control measures to further ensure the integrity, accuracy, and currency of data in its consolidated terrorist screening database. We all remember when travelers named "David Nelson" had difficulty at airline check-in because another person with that same name was on a watchlist. With the ability to authenticate the identification of most passengers, and with the improved system and procedures the TSC is implementing, we expect CAPPS II will greatly reduce the number of these "false positives."

TSA plans to test CAPPS II prior to its deployment to demonstrate its effectiveness, and to refine the operations and the redress mechanisms we are building. To date, individual airlines are reluctant to provide the Government with the necessary PNR information to enable us to test the system due to both public concerns over privacy questions and legal considerations. We understand these concerns, and are working on alternative solutions that may help us obtain limited data for testing. We are committed to providing the same degree of privacy protection for any test or full system PNR data use. Additional work in this area remains to be done before such an order or regulation would be issued, and we will keep this Subcommittee apprised of our progress.

The recent GAO report, released on February 13, 2004, responded to requirements set forth in the Homeland Security Appropriations Act, 2004 (P.L. 108-90). GAO generally concluded that in most areas that Congress asked them to review, our work on CAPPS II is not yet complete. DHS has generally concurred in GAO's findings, which in our view confirm that CAPPS II is a program still under development. As discussed earlier, the reluctance of air carriers and passenger reservation systems to provide TSA with critical

PNR data, and ongoing but unresolved discussions with organizations like the European Union (discussed below), have hampered our ability to move forward with the necessary testing. As we resolve the issues of access to PNR data, and the testing phase moves forward and results in a more mature system, we are confident we will be able to satisfy the questions Congress posed.

The GAO report did however fail to note that, notwithstanding the inability of TSA to test the system with PNR data, we have made substantial progress in development. CAPPS II has a baseline functioning system that has been tested using simulated PNR data from volunteer employees. Presently, CAPPS II modules can receive simulated PNR data through the Airline Data Interface (ADI), standardize and format the data, and transmit the formatted data through the identity authentication process. Further, CAPPS II is capable of conducting a basic risk assessment and receiving an authentication score. It has undergone integration testing to ensure that the modules can work together. Additional testing phases will verify that the system is functional, that it can process the large volume of air travelers, meet a desired turnaround time, and produce a risk assessment, resulting in a recommended screening level for each passenger.

We have also received significant cooperation from foreign governments who have embraced the concept of a robust passenger prescreening system. We are engaged in intensive discussions with the European Union (EU) regarding the delivery of PNR data from citizens covered by the EU. The members of the EU are very sensitive to the privacy concerns of their citizens, and we share their concerns. However, as continually demonstrated by threats against commercial airlines from certain international locations, we must collectively find a solution. The continual cancellation of certain flights of interest is one method of handling these threats. More effective prescreening of passengers is another, far less costly way.

There has been continuing concern about expanding "the mission" of CAPPS II -- that is, using the system in areas for which it was never intended. I earlier mentioned using CAPPS II to identify travelers with outstanding warrants for violent criminal behavior. Our Interim Privacy Act Notice, published in August 2003, made it clear that we would consider the ability of CAPPS II to identify individuals with outstanding warrants for federal or state crimes of violence. We believe that it is entirely appropriate to bring such individuals to the attention of law enforcement officers. A person fleeing from justice for a violent crime should not be able to use the aviation system to escape from justice. Again, this is an area where misinformation abounds. A passenger with unpaid parking tickets or an outstanding civil judgment is not a person subject to an outstanding warrant for a violent crime. Nor would this component of a CAPPS II assessment prevent air travel by people who have paid their debts to society. Nevertheless, our design work continues to clarify and narrow the amount of information collected, how the information may be used, the length of time the information may be retained, and the parties with whom information may be shared. Any and all changes will be published in the Final Privacy Act Notice.

Another area of concern revolves around the growing area of identity theft. Many have asked whether an individual who has stolen another person's identification can thwart CAPPS II by posing as the innocent victim. To answer this question, it is important to point out that because one of the primary functions of CAPPS II is to verify the identities of air travelers. Passengers making airline reservations must provide information that matches information contained in commercial databases. Frequently, those who commit identity theft change such information (*i.e.* home telephone number or home address), in order to perpetrate the fraud, receive credit cards that the victim never applied for, and avoid detection. The sophisticated methodologies used by the commercial sector that we are working to harness with the CAPPS II system are very likely to flag this anomaly. As we move toward testing CAPPS II with real PNR data, we will have a much better view of how well CAPPS II discerns legitimate travelers from those who have stolen an innocent person's identity, and seek to travel on commercial aircraft.

Mr. Chairman, CAPPS II remains a high priority for TSA, and we believe it will be an essential element of aviation security. We appreciate the support that you have voiced for quick implementation of CAPPS II. However, we are also much aware of the privacy concerns of many American citizens and our foreign counterparts, and the need to adequately educate the American public and others concerned about what CAPPS II will do and what it will not do. We are heavily engaged in resolving these concerns and look forward to your continued support and that of the Congress.

I will be pleased to answer any questions that you may have.

House Committee on Transportation and Infrastructure
Subcommittee on Aviation
“The Status of the Computer-Assisted Passenger Prescreening System
(CAPPS II)”
March 17, 2004

Questions from Rep. Shelley Berkley

1. I first want to thank you for working with McCarran Airport to improve the situation at the security checkpoints. As you know, McCarran is second only to Los Angeles International Airport in the number of origination and destination passengers. Do you think that the CAPPS II system will help speed up the process at security checkpoints?

Answer: A decision was made in 2004 not to proceed with the CAPPS II proposal. On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger prescreening program called Secure Flight. Under Secure Flight, the Transportation Security Administration (TSA) will take over from the air carriers responsibility for the comparison of domestic airline Passenger Name Record (PNR) information against terrorist watchlists. Secure Flight will use records contained in the consolidated Terrorist Screening Center Database (TSDB), to include the No-Fly and Selectee lists. Secure Flight will meet the Department's goals of improving the security and safety of travelers on domestic flights, reducing passenger airport screening time, and protecting privacy and civil liberties.

The new Secure Flight program is designed to improve the efficiency of the prescreening process and reduce the number of people selected for secondary screening. TSA will be able to use the consolidated watch lists contained in the TSDB, including the expanded No Fly and Selectee lists. Consolidating these checks within the Federal Government will allow TSA to automate most watch list comparisons and apply more consistent internal analytical procedures when automated resolution of initial "hits" is not possible. It will help eliminate false positive watch list matches, improve passengers' experience under the existing system by helping move passengers through airport screening more quickly, reduce the number of individuals selected for secondary screening, and allow for more consistent response procedures at airports for those passengers identified as potential matches. Consequently, TSA will be able to concentrate its screening resources more efficiently.

TSA recently completed the initial round of effectiveness testing with historical PNR data to determine which items of passenger information are most effective in matching against the watch list while yielding the lowest number of false positive or negative matches. TSA will incorporate the results of the test in support of program development. Consistent with the

National Intelligence Reform and Terrorism Prevention Act of 2004, TSA will begin implementing Secure Flight in August 2005.

2. Prior to New Year's Eve this year, hotels in Las Vegas were required to release their guest lists to the FBI and there was a great deal of concern about the privacy of our visitors. What assurances do we have that the information collected by the CAPPS II system will only be used to identify potential terrorist threats and that the privacy of law abiding citizens will be protected?

Answer: A decision was made in 2004 not to proceed with the CAPPS II proposal. On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger prescreening program called Secure Flight.

To protect passengers' personal information and civil liberties, Secure Flight will:

- Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for secondary screening or they are having a difficult time obtaining boarding cards.
- Build in implementation of the Department of Justice's Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (June 2003) by avoiding the use of generalized stereotypes regarding race or ethnicity in selection, consistent with the Guidance.
- Comply with Privacy Act requirements.

TSA is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening. The TSA Office of Civil Rights or TSA Privacy Officer will make initial determinations, and an appeals process will allow for review by the DHS Officer for Civil Rights and Civil Liberties and/or the DHS Chief Privacy Officer.

House Committee on Transportation and Infrastructure
Subcommittee on Aviation
“The Status of the Computer-Assisted Passenger Prescreening System (CAPPS II)”
March 17, 2004

Questions from Rep. Eddie Bernice Johnson

1. Admiral Stone, it is my understanding that TSA plans to destroy most passenger information shortly after they have completed their travel itinerary. How long will the information be retained? Will this be sufficient time for a passenger to be able to challenge their security risk or authentication score?

Answer: TSA has submitted a proposed retention schedule to the National Archives and Records Administration (NARA) requesting a short retention period of 72 hours. In establishing a policy for retention, TSA is taking into consideration any requirements necessary to facilitate the redress process where passengers believe they have been unfairly or incorrectly identified for additional screening

2. Does TSA plan to retain CAPPS II information long enough to assess if there is disparate impact of the system on particular religious and ethnic groups? If not, will there be some measure in place to assess disparate impact?

Answer: A decision was made in 2004 not to proceed with the CAPPS II proposal. On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger prescreening program called Secure Flight. Under Secure Flight, the Transportation Security Administration (TSA) will take over from the air carriers responsibility for the comparison of domestic airline Passenger Name Record (PNR) information against terrorist watchlists. Secure Flight will use records contained in the consolidated Terrorist Screening Center Database (TSDB), to include the No-Fly and Selectee lists. TSA recently completed the initial round of effectiveness testing with historical PNR data to determine which items of passenger information are most effective in matching against the watch list while yielding the lowest number of false positive or negative matches. TSA will incorporate the results of the tests in support of Secure Flight program development. Consistent with the National Intelligence Reform and Terrorism Prevention Act of 2004, TSA will begin implementing Secure Flight in August 2005.

Secure Flight will not consider racial or ethnic stereotypes as the basis for selection, consistent with the Department of Justice’s Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (June 2003). Reliance on generalized stereotypes is forbidden. To ensure the respect for travelers’ civil rights, the DHS Office for Civil Rights and Civil Liberties and TSA Office of Civil Rights will be integrated into the redress appeals process.

TSA believes that the improper use of profiling is inconsistent with American ideals. Furthermore, it is ineffective in detecting or deterring terrorists because focusing screening efforts on something so obvious as race or ethnicity would give terrorists an easy way to avoid detection—by simply recruiting terrorists of a different race, religion, or ethnicity.

In order to measure disparate impact accurately, information about the race, ethnicity, religion, and other features of the air traveling public would need to be available and compared against similar information for individuals who are selected for enhanced screening by the proposed Secure Flight system. Secure Flight as designed will not have documented information such as the race, ethnicity, or religion of the air traveling public, and, therefore, will not be a source of information to measure disparate impact on such grounds. In addition, to our knowledge, there is no independent, verifiable source of general information regarding the religious or ethnic composition of the air traveling public.

TESTIMONY OF THE
THE AMERICAN SOCIETY OF TRAVEL AGENTS, INC.
Before the
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON AVIATION
“Status of The Computer-Assisted Passenger Prescreening System
(CAPPS II)”

Presented by:

Paul M. Ruden, Esq., CTC
Senior Vice President – Legal & Industry
Affairs
American Society of Travel Agents, Inc.
1101 King Street
Alexandria, VA 22314
(703) 739-2782
pruden@astahq.com

March 29, 2004

Testimony of the American Society of Travel Agents

The American Society of Travel Agents ("ASTA") offers this testimony on the Subcommittee's deliberations on the state of the Computer-Assisted Passenger Prescreening System known as CAPPs II.

We have read with special interest the testimony of two witnesses at the public hearing on March 17, 2004. One was Mr. James May, President & CEO of the Air Transport Association of America (ATA) to the effect that any new CAPPs II rule must require that third parties (meaning travel agents) collect the needed information "at the time of their first contact with the customer."¹ The other was the statement of Acting Administrator of the Transportation Security Administration, David M. Stone, telling this Subcommittee that "Currently, the CAPPs II system is being designed to perform the following functions: "Obtain available Passenger Name Record (PNR) data from airlines and computer reservation systems. At a minimum this data will include full name, home address, home telephone number, and date of birth."²

Given the central role that travel agents (traditional and online) continue to play in the promotion and sale of air transportation in the United States, there is little question that they will have a critical place in the implementation of any new passenger security rule derived from passenger reservation information. There are, however, very serious questions about adopting a rule, whether federally imposed or airline imposed, requiring travel agents to collect specific information from prospective passengers "at the time of their first contact with the customer," as proposed by ATA. In the first instance, the collection, retention and transmittal of any additional PNR information is going to require basic changes in the displays and back-office system-interaction programming of the computer reservation systems. Absent such changes, there is no practical possibility that travel agents can comply with any mandates to collect and deliver additional PNR information.

Beyond that, there is a telling uncertainty in the testimony of Mr. Stone, suggesting that CAPPs II may require still more information than is now popularly believed to be the destiny of the CAPPs II program. The familiar rubric "name plus three" has not been

¹ Statement of James C. May, President & CEO of the Air Transport Association of America, Inc., March 17, 2004 at p. 6.

² Statement of David M. Stone, Acting Administrator, March 17, 2004, at p. 3.

established anywhere with finality. It is, therefore, impossible for anyone in the industry to engage in meaningful analysis of what changes in business practices and computer programming are required to accommodate the CAPPs II system.

ASTA has been trying, with others in the retail industry, for a very long time to engage TSA in a meaningful dialogue about the scope and content of CAPPs II. Our efforts have resulted in a few preliminary meetings, but while substantive dialogue has been promised repeatedly, no such interaction has occurred and as of this writing none has, to our knowledge, been scheduled.

ASTA has been making these efforts for three related reasons. One is that it is in the interest of the people we represent, because their businesses will be directly and dramatically affected by any foreseeable CAPPs II rule. The second reason is that we seek to assist the government in developing an improved security system that will encourage people to travel because they feel safer and experience fewer hassles and delays at the airport. The third reason is that improved security is in the national interest and ASTA supports all efforts to protect the homeland from those that would destroy it through violence or intimidation directed at our people or the economy.

In short, we have sought to be a "friend" to CAPPs II by offering to help shape a rule that enhances security without defeating the willingness of people to travel and without impairing the already fragile economics of retail travel distribution which continues to serve the vast majority of air travelers in this country. At present, however, it appears that we will end up in the growing army of parties who will be objecting to the proposed CAPPs II rules, because they will not be based on a deep understanding of the way the travel business is sold at retail and the possible cost and other implications, including suppression of travel demand, that may ensue. ASTA will aggressively resist any rules that impose unnecessary costs on travel retailers or create unnecessary further obstacles to facilitation of the travel experience. Conflict of this kind could probably be avoided if TSA would engage ASTA, and others, in a meaningful pre-proposal dialogue about the content of the proposed rules. We ask this Subcommittee to use its influence with TSA to bring about meaningful pre-proposal dialogue with key industry groups, including ASTA, the GDS's and others.

Respectfully submitted.

Paul M. Ruden, Esquire
Senior Vice President
Legal & Industry Affairs
American Society of Travel Agents, Inc.
1101 King Street

Testimony of

**Nancy K. Holtzman
Executive Director
Association of Corporate Travel Executives**

**Regarding The Deleterious Impact of CAPPS II
on the Business Travel Industry**

**To the U.S. House of Representatives
Transportation and Infrastructure Committee
Subcommittee on Aviation,
Hearings on The Status Of The Computer-Assisted Passenger
Prescreening System (CAPPS II)**

March 17, 2004

Chairman Mica and members of this distinguished Committee; I appreciate this opportunity to present the views of the Association of Corporate Travel Executives regarding the potentially deleterious impact of CAPPS II on the business travel industry. As you are aware, the economic contribution of business travel, and its role in both the national and global recovery is very significant.

The Association of Corporate Travel Executives represents the safety, security, and service interests of a million business travelers, and the financial concerns of more than 900 major corporations in all 50 states and 37 countries across the globe -- as well as the welfare of the traveling public in general. Our U.S. membership is comprised of a major cross section of industrial America, including defense contractors, the energy industry, the banking community, heavy manufacturers, major educational institutions, communications firms, prominent pharmaceutical houses, and light manufacturers.

ACTE members' companies have hundreds of thousands of travelers in the air on any given day. We represent billions of dollars in travel-generated taxes and many times that in direct expenditures, which support the heart of American commerce. Even by a conservative estimate, this trickle down affect of ACTE members on the overall American economic infrastructure cannot be measured in dollars alone, but in jobs, corporate growth potential, company reinvestment, and ultimately -- share value. The business traveler is a critical part of the nation's -- and the world's-- economic future. And the successful, seamless flow of business travel is critical to the American business profile.

The Association of Corporate Travel Executives fully understands the necessity of protecting air travel as a strategic U.S. asset. We support any realistic effort to make air travel safe and as invulnerable to terrorist attack as humanly possible. We recognize the challenges and efforts of the Transportation Safety Administration to devise an automated screening system that is racially impartial, automatic in its operation, and impervious to tampering. Yet we believe the premature and unrealistic implementation of

the current Computer Assisted Passenger Prescreening System (CAPPS II) may end up costing the business travel industry billions of dollars by failing to address fines, ticket penalties, trip cancellations, and manpower hours lost – without even the basic consideration of a passenger resolution process.

Mr. Chairman, the focus of the media and other organizations regarding CAPPS II has been primarily on the question of personal privacy and the perceived loss of individual freedoms. You will hear enough on this emotionally charged subject throughout these hearing. Likewise, distinguished experts on personal freedoms can easily make the case that CAPPS II can be extended into every aspect of American life from the purchase of train tickets to real estate (in an attempt to establish baseline residency).

Our case is far more direct. The impact of CAPPS II on the business travel industry needs no hypothetical extrapolation. Through analysis and study, our association has determined that as it stands, CAPPS II treats delays, the potential for trip cancellation, and the resulting charges (flights missed, meetings canceled, and the cost of unused surface and air transportation) as incidental -- something that will be eventually addressed in some manner, after the program is implemented.

This approach is unacceptable to Corporate America, who will undoubtedly bear the brunt and expense of the charges, and ultimately the cost of lost business productivity.

How high will these charges be? Our estimation of the figure is based upon the number of travelers the TSA -- or other authorities -- claims will be either delayed for further interrogation or denied boarding. Using conservative estimates of one to 2 percent of the overall travel figure of 400 million, this presents the industry with between 4 and 8 million passengers that will be detained or denied boarding. Assuming that one to two million of these will be business travelers, resulting costs generated by ticket penalties, missed meetings and canceled support arrangements might run as high as \$2 billion.

But the cost to industry will go far beyond the charges associated with travel. In a study quoted by Daniel Goldman in his book "Working with emotional Intelligence, it is estimated that salesman for Fortune 500 firms generate an average of \$3 million per year in sales. That's over \$11,500 per day and over \$1,400 per hour. How can corporate America reclaim the value of those lost hours and the opportunity cost of lost business.

Avoiding or minimizing these impacts on business, will require a resolution process that works as fast as getting passenger tagged with false-positive readings back on the plane as quickly as they were removed. It will require a resolution process that is designed by TSA with input and involvement from major travel industry stakeholders, such as ACTE, rather than designed in a vacuum and proved unworkable when implemented. The potential costs are much too high to risk failure.

Furthermore, ACTE's CAPPS II task force has determined that the basic operating principle of this program is in direct conflict with privacy policies of most major American corporations. Complying with CAPPS II may expose these corporations to liability and litigation stemming from compromised passenger record numbers (PNR data) or stolen identities resulting from unauthorized access to records. The combination of additional travel charges, lost corporate revenue, and the threat of corporate litigation may force companies to invest more heavily in alternatives to business travel.

We respectfully recommend the following steps be taken:

It is the opinion of our membership that CAPPS II -- nor any program like CAPPS II -- should not be submitted for consideration until all of these provisions are provided for in a detailed plan.

1. The CAPPS II program should not be submitted for consideration -- let alone implementation -- until it contains a cost impact analysis detailing charges to the carriers, the GDS systems and to companies (in manpower hours, fines, and penalties due to delays and lost opportunities).
2. All pressure should be taken off the airlines to supply the federal government with PNR's until an exact process -- that complies with security requirements, corporate privacy policies, and resolution issues -- is developed.
3. Every effort should be made to involve the major stakeholders in the CAPPS II development process. The TSA should expand its briefings with business travel industry leaders to include focus groups to help devise mechanisms like a speedy resolution process, ways to work with GDS companies, and gauging the impact on corporate privacy policies, before announcing proposed testing dates for CAPPS II. Fully detailed fines schedules and current procedures should be published for the traveling public immediately.
4. Full funding for CAPPS II should not be granted until DHS and TSA satisfactorily resolve the seven CAPPS II issues identified by Congress as key areas of interest and determined by the GAO as yet to be addressed.

In conclusion, the Association of Corporate Travel Executives would like to thank Chairman Mica and this committee for responding so quickly to an issue that will have long-term implications for corporate America, the traveling public, and the national economy. The resources of our association are at the disposal of this committee and the TSA.

Thank you.

Testimony of
The Business Travel Association of Germany
Regarding CAPPS II
Before the U.S. House of Representatives
Transportation and Infrastructure Committee
Subcommittee on Aviation
March 17, 2004

The Business Travel Association of Germany (VDR) observes with concern the recent developments in U.S. travel regulations. We welcome all sincere efforts to establish better security measures but also see the need to implement policies, programs and practices which are in accordance with EU rights and civil liberties and do not burden business travellers and their companies with unnecessary costs.

Even some of the present procedures are simply detrimental to international trade and travel. VDR members who export machinery to the U.S. report, that they are unable to obtain adequate visa for their trouble-shooting mechanics. U.S. authorities are reported to ignore German arguments which have resulted in the fact that some frustrated companies now seek legal help. It would be totally intolerable if new trade obstacles would be introduced camouflaged as travel security measures.

We are aware that not all single concerns and questions can be presented in such a testimony. One of the details we wonder about e.g. is: If a business traveller, who travels with colleagues or in a group, is marked "yellow", does this influence the security status of his or her fellow travellers?

VDR is eagerly awaiting a government testimony in the Federal Parliament in Berlin concerning U.S. travel regulations. The information requested include details about the PNR information exchanged between German and U.S. authorities and/or carriers, the legal and cost effects of CAPPS II on travel managers and travel agents, the legal status of travellers who are (innocently) charged with security matters, the question of responsibility for damages and more. We hope this will bring more light into those matters which are of special interest to non-U.S. travellers.

VDR will evaluate these further insights and suggest to Paragon a resolution for the meeting on March 31st in Wales.

VDR is also preparing a statement for the Federation of German Industries (Bundesverband der Deutschen Industrie, BDI), directed at the U.S. Board of the BDI Board. The U.S. Board has already voiced its concerns in a paper which German Chancellor Gerhard Schroeder has touched upon during his visit in the USA on February 26-28. The paper stresses the fact that combating terrorism is an international effort. Any measures taken should not unduly strain economy and trade. It is vital to intensify transatlantic cooperation with timely participation of the economy to avoid over-regulation, protectionism and unilateralism. Dr. v. Wartenberg, Senior Director of BDI, will travel to the USA in May and push the BDI's point of view.

###

About VDR:

The Business Travel Association of Germany was established in 1974 and has more than 400 member companies with a combined annual turnover in corporate travel of € 9 billion.

Testimony of
The Institute of Travel Management
Regarding CAPPS II
Before the U.S. House of Representatives
Transportation and Infrastructure Committee
Subcommittee on Aviation
March 17, 2004

The Institute of Travel Management (ITM) fully supports the Business Travel Coalition's stance on Computer Assisted Passenger Pre-Screening System (CAPPS II) and the testimony of its chairman Kevin Mitchell.

As the professional association representing the business travel managers, buyers and suppliers in the UK and Ireland, ITM views the issue of data protection and civil liberties with great concern. However the prospect of increased prices and delays to flights are also of concern to our members. Traveller security is vitally important and must be taken as a given by those who fly, nevertheless in a recent study undertaken by ITM, 1 in 5 members felt that the benefits of enhanced security are cancelled out by the disadvantages of increased costs and delays. Travel management companies and other distribution businesses face unknown costs to reconfigure their systems in accordance with the requirements of CAPPS II and ITM believes that it is inevitable that these costs will in turn be passed onto the customer.

ITM first expressed severe reservations when PNRs were introduced in 2003. PNRs provide yet another opportunity for travel data to be leaked to undesirable recipients. Furthermore a convincing explanation has yet to be made about how exactly PNR data will help combat terrorism. Finally, the European Commission has also expressed concern that the US has taken unilateral action on a global aviation issue instead of through an appropriate authority such as the International Civil Aviation Organisation.

Although at this time the final form CAPPS II is unclear, ITM notes that US carriers are withdrawing support from the trial use of PNR data as part of the scheme. Travellers are rightly unhappy that the trials were conducted without their knowledge and that at least one airline had released PNR's despite initially denying that they had done so. All airlines and/or agents should be informing passengers what is happening to PNRs to allow the passenger to make an informed decision to accept the situation or not to fly to the USA.

###

Institute of Travel Management
 34 Chester Road
 Macclesfield
 Cheshire
 United Kingdom
 SK11 8DG
 Tel: +44 1625 430472

THE PRACTICAL NOMAD

EDWARD HASBROUCK

1130 Treat Avenue, San Francisco, CA 94110, USA

phone +1-415-824-0214

edward@hasbrouck.org

<http://hasbrouck.org>

The Practical Nomad: How to Travel Around the World (3rd edition, 2004)

The Practical Nomad Guide to the Online Travel Marketplace (2001)

<http://www.practicalnomad.com>

**Testimony for the record of the hearing
before the U.S. House of Representatives
Committee on Transportation and Infrastructure
Subcommittee on Aviation
17 March 2004
"The Status of the Computer-Assisted
Passenger Prescreening System (CAPPS-II)"**

Dear Chairman Mica, Ranking Minority Member DeFazio,
and members of the Subcommittee:

As the leading industry expert and consumer advocate on CAPPS-II, I thank the Subcommittee for holding this hearing on "The Status Of The Computer-Assisted Passenger Prescreening System (CAPPS II)", and for the opportunity to submit this written testimony.

The recent GAO report on CAPPS-II has only begun to scratch the surface of the cost and implementation burden that will be imposed on tens of thousands of travel agencies (mostly small family businesses) as well as airlines, reservations services, and providers of reservation software.

The GAO report noted that. "According to the draft Business Case for CAPPS II, the system has an estimated life cycle cost of over \$380 million through fiscal year 2008," but noted that, "Life cycle costs do not include air carrier, reservation company, or passenger costs." The GAO was not charged with, and did not conduct, any further investigation of those future costs, which the travel industry will undoubtedly ask Congress to underwrite and/or reimburse.

According to the GAO report, the TSA has been relying entirely on assumptions about the content of airline reservations based on a sample of only 32 reservations, which is inadequate as a basis for any meaningful understanding or budgeting.

It's critically important for the Subcommittee to understand the cost and privacy implications of the changes in travel industry information technology infrastructure and business procedures that the TSA proposes to require -- *before* proceeding further with proposals that may be impossible or unaffordable to implement in the manner currently conceived by the TSA.

More than a year ago, in my comments on the first Privacy Act notice by the DOT for CAPPS-II, I estimated those costs to industry -- none of which have yet been included in the TSA's budget projections for CAPPS-II -- as likely to exceed US\$1 billion. I also discussed in detail the particular privacy and policy problems inherent in reliance on commercial reservation networks, and a chain of multiple intermediaries, to collect the additional data the TSA proposes to require for CAPPS-II.

Unfortunately, the second Privacy Act notice by the DHS for CAPPS-II not only expanded the data proposed to be required (contrary to the claims by the DHS and TSA to have "narrowed" the data to be used by CAPPS-II) but failed in its purported "analysis of comments" even to acknowledge, much less respond to, any of the comments objecting to the first CAPPS-II notice on the grounds that it is unconstitutional; that it violates the right to travel; that it exceeds the claimed statutory authority; that it failed to include the required economic and small business impact assessments; that it is incompatible with the privacy laws of major air transportation partners of the USA, including the European Union and Canada; and that it failed to satisfy the statutory notice and comment requirements (particularly in failing to identify the many categories of individuals other than passengers about whom airline reservations contain personal information, and failing to specify adequately either what data would be required of whom and when, or the penalties for not providing this).

At the heart of CAPPS-II is the data contained in airline reservations, and at the center of the privacy debate over CAPPS-II is how that reservation data is handled, both by commercial entities and government agencies. These issues have not yet been addressed, and should be.

More than a year after the close of the first comment period, and six months after the close of the second, the DHS still has not even made public the complete record of comments it received, despite conceding that it was the largest number of comments ever received by any agency on a Privacy Act notice.

More importantly, the DHS still has not acknowledged the issues raised by those comments; conducted the requisite economic, small business, and privacy impact assessments; or issued a notice satisfying the requirements of the Privacy Act.

Since the DHS has not dealt with these issues, and since many of them are outside the scope of the investigation the GAO was directed to conduct, it remains the responsibility of this Subcommittee, and the Congress, to conduct its own *de novo* investigation of the economic and privacy impacts of CAPPs-II.

Many of the cost and implementation questions concerning CAPPs-II which have been mentioned in the testimony of other witnesses were first raised in my investigative reporting and consumer advocacy, through my articles, newsletter, Web site, and blog, and in my comments on the CAPPs-II Privacy act notices.

Since those remain the key issues for the Subcommittee, and have not yet been dealt with by the DHS or TSA, I have attached my comments on the two CAPPs-II Privacy Act notices for inclusion in this record, and for the Subcommittee's use in evaluating the likely cost of CAPPs-II, its economic and privacy impact, the validity of the Privacy Act notices, and the desirability of continued testing, development, and deployment of CAPPs-II.

Sincerely,

Edward Hasbrouck

Enclosures:

Comments Re: Docket Number DHS/TSA-2003-1, Passenger and Aviation Security Screening Records (PASSR), 30 September 2003 (pp. 1-29)

Comments Re: Establishment and Exemption from the Privacy Act of Records System DOT/TSA 010, Aviation Security-Screening Records (ASSR), 23 February 2003 (pp. 30-54)

Written Statement
of
Deborah Pierce, Executive Director
Linda Ackerman, Staff Counsel
PrivacyActivism
to
House Committee on Transportation and Infrastructure
Aviation Subcommittee
“Status of the Computer-Assisted Passenger Pre-screening System (CAPPS II)”
March 25, 2004

Mr. Chairman and Members of the Subcommittee:

PrivacyActivism, along with the Electronic Frontier Foundation (EFF), Privacy Rights Clearinghouse, and Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), submitted detailed comments concerning their opposition to the CAPPS II passenger screening system last September, in response to the Transportation Security Administration's (TSAs) August 1, 2003 interim final notice and notice of status under the Privacy Act of 1974 (Docket Number DHS/TSA-2003-1). Our comments are posted at http://www.eff.org/Privacy/cappsii/20030930_comments.php.

The following points are a high-level summary of our objections to CAPPS II:

- CAPPS II will likely be ineffective at stopping terrorists.
- CAPPS II and the secrecy surrounding its risk assessment procedures will threaten travelers' constitutional rights, including the right to travel, to speak and associate freely, and to be free from unreasonable searches and seizures.
- CAPPS II, by failing to satisfy the statutory requirements of the Privacy Act of 1974 or to comply with Fair Information Practices, will violate travelers' privacy.
- CAPPS II, if implemented, will be used for purposes other than preventing terrorism.

CAPPS II Can Only Be As Effective As the Data It Depends on Is Accurate

Rather than reiterate objections we have already made, we are submitting these written comments to the Aviation Subcommittee to raise an additional matter that we believe is the Achilles heel of the proposed passenger screening system. That is, the accuracy of the data that will be used to verify individual identity and to create profiles that will determine who is a risk to aviation security, and how the current epidemic of identity theft impacts that data.

Even before CAPPS II is operation, it is obvious that the effects of incorrect data have already been assigned a very low priority in developing the system. This is apparent because:

1. There is no requirement that the commercial databases that will be used to verify identity and will likely be used in the profiling process be accurate.
2. In March 2003 the Attorney General issued a rule exempting the National Criminal Information Center database from the 1974 Privacy Act's requirements for accuracy and timeliness of information. 68 Fed. Reg. 14140 (Mar. 24, 2003) (codified as 28 C.F.R. 16)

The question of data accuracy links the goal of CAPPS II—identifying people who represent a threat to aviation security—with the bedrock principle of binary operating systems. If you give the system incorrect information to sort, you will get incorrect results.

Rampant Identity Theft Will Compound Inherent Data Inaccuracies

A report issued by GAO in February 2004 titled "Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Challenges" expresses the concern that the TSA has not ensured the accuracy of the data that CAPPS II will use to identify and profile passengers. <<http://www.gao.gov/new.items/d04385.pdf>> We share that concern. We also strongly doubt that it is even possible to maintain a level of accuracy that would yield an "acceptable" rate of error—if there is such a thing. Inevitable false conclusions about individual threat ratings—both positive and negative—will arise from mistyped social security numbers and surnames. Another factor that has major implications for creating corrupt data, which has not even been taken into account, is the effect of rampant identity theft.

According to the Bureau of Transportation Statistics (BTS), there were approximately 587 million domestic airline passengers in 2003. The Washington Post reported in September 2003 that the TSA estimated that CAPPS II would flag 8% of passengers as yellow for further checking and 1-2% as red for no-fly.

<<http://www.washingtonpost.com/wp-dyn/articles/A45434-2003Sep8.html>>

The FTC Report on Identity Theft Should Be Seriously Considered in Assessing the Issue of Data Accuracy in CAPPS II

Also in September 2003, the Federal Trade Commission released a study showing that 27.3 million Americans had been victims of identity theft since 1998, including 9.9 million people in 2003 alone. <<http://www.ftc.gov/os/2003/09/synovatereport.pdf>> While certainly not all instances of identity theft will affect the profile constructed in a passenger risk assessment, the sheer number of records that will contain corrupt data as a result of ID theft is staggering.

The FTC report states that 4% of identity theft victims had their name and personal information wrongly given to law enforcement when a crime was committed.¹ This information misconnecting someone with a crime will become part of the FBI's NCIC database. It will be a crucial factor in assessing passenger risk. Even if only a small percentage of people affected by criminal ID theft are wrongly associated with violent crimes, they have the potential to become a large number of people incorrectly flagged by CAPPS II as violent felons and threats to aviation security. Those wrongly connected to lesser crimes will be noted as suspicious and will face stricter security procedures whenever they fly.

An additional 4.7% of those surveyed for the FTC report said that their personal information had been used to open new accounts, take out loans, or commit unspecified theft or fraud.² This is the type of information that will end up in databases held by private aggregators, which the TSA intends to use to verify a passenger's identity against the airline PNR (passenger name record) information collected at the time someone makes a reservation. The TSA has not acknowledged that it will also use private aggregator information for predictive modeling about behavior and to determine such characteristics as "rootedness" in the community, but it is very likely that it will do so. The types of transactions done with stolen identities could easily be among those that will raise suspicions about a person's behavior, but based on the FTC's identity theft numbers, how many of them will associate the wrong person with suspicious behavior?

Conclusions

The GAO report found that the TSA had not done enough to ensure accuracy of information in the databases it will use to assess risk. Taking into account, however, the epidemic of identity theft in this country, and how the misinformation it creates will be absorbed into the databases CAPPS II will use to determine who is a threat to aviation security, how will it even be possible to ensure a reasonable level of accuracy in the proposed passenger screening system?

For this reason alone we believe that CAPPS II should not be implemented. It presents an enormous threat of wrongly branding innocent people who are the victims of identity theft as criminals and possibly as terrorists.

Respectfully submitted,

Deborah Pierce, Executive Director
Linda Ackerman, Staff Counsel
PrivacyActivism
4026 18th St.
San Francisco, CA 94114

¹ Federal Trade Commission – Identity Theft Survey Report, p. 6

² *Id.*, at p. 11